AFRL-RI-RS-TR-2013-123

STATE UNIVERSITY OF NEW YORK INSTITUTE OF TECHNOLOGY (SUNYIT) VISITING SCHOLARS PROGRAM

RESEARCH FOUNDATION FOR SUNY (RF)

MAY 2013

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2013-123 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /

FRANKLIN E. HOKE, JR
Work Unit Manager

/ S /

MARGOT R. ASHCROFT
Chief, Strategic Planning
and Integration Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
MAY 2013	FINAL TECHNICAL REPORT	APR 2011 – MAR 2013

4. TITLE AND SUBTITLE

STATE UNIVERSITY OF NEW YORK INSTITUTE OF TECHNOLOGY (SUNYIT) VISITING SCHOLARS PROGRAM

5a. CONTRACT NUMBER
FA8750-11-2-0218

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
62788F

6. AUTHOR(S)

Deborah J. Tyksinski

5d. PROJECT NUMBER
B201

5e. TASK NUMBER
1S

5f. WORK UNIT NUMBER
UN

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Research Foundation for SUNY (RF)
SUNYIT
100 Seymour Road
Utica NY 13502

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIBA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2013-123

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

RF for SUNY (SUNY/IT) has contributed significant research capability and capacity to the in-house program at AFRL through the placement of highly motivated and accomplished faculty members and graduate students pursuing advanced degrees in Engineering, Computer Science, Mathematics and other recognized technical disciplines critical to the advancement of information technologies. SUNY/IT worked closely with AFRL to help build, foster and nurture in-house research terms. Under this effort SUNYIT recruited, placed and supported administrative requirements for 48 faculty members and 36 undergraduate/graduate research assistants and coordinated an additional 42 faculty extension efforts.

15. SUBJECT TERMS

Cloud Computing, Physics, Electrical Engineering and Computer Science

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**FRANKLIN E. HOKE, JR.**
U	U	U	SAR	54	19b. TELEPONE NUMBER (*Include area code*) **315-330-3470**

TABLE OF CONTENTS

1. INTRODUCTION 1
2. FACULTY & RESEARCH AREAS 2
   2.1. 2011 Summer Faculty 2
   2.2. 2012 Summer Faculty 12
3. CONTINUING RESEARCH PROJECTS 25
   3.1. 2011 Faculty Extension Grants 25
   3.2. 2012 Faculty Extension Grants 31
4. EXPENDITURES 46
   4.1. Faculty Labor 46
   4.2. Other Costs Associated with Program 46
5. LIST OF ACRONYMS 47

1. INTRODUCTION

The Research Foundation, for and on behalf of SUNY Institute of Technology (SUNYIT), has contributed significant research capability and capacity to the in-house program at AFRL through the placement of highly motivated and accomplished faculty members and undergrad/graduate students pursuing advanced degrees in Engineering, Computer Science, Mathematics and other recognized technical disciplines critical to the advancement of Information Technologies. The program supported and enhanced the existing AFRL/Information Institute Visiting Faculty Research Program and the AFOSR Summer Faculty Fellowship Program.

SUNYIT worked closely with AFRL to help build, foster, and nurture in-house research teams. Under this effort SUNYIT recruited, placed and supported administrative requirements of faculty members and undergrad/graduate research analysts and coordinated additional faculty extension efforts.

2. FACULTY & RESEARCH AREAS

2.1. 2011 Summer Faculty

Bharat Bhargava - Security Properties of A Managed Information Object (MIO) in a Peer to Peer Environment with Publish and Subscribe Paradigm; Computer and Computational Science Dept, Purdue University

Research was conducted in studying the security properties of a managed information object (MIO) in a Peer to Peer environment with publish and subscribe paradigm. The parameter for formalizing privacy, data leakage, policy enforcement and trust were identified and explored. Contributions were made to advancing security and privacy in cloud environment. A set of tutorial slides were developed to identify problems and current approached. The ideas of active bundles (AB) and its relationship with MIO were developed. A prototype of AB is being extended to conduct experiments to that can shed lights on the security properties of MIO.

We worked with scientists in Cross-domain information exchange in AFRL and developed ideas that can be useful for dissemination of data in various security clearance levels. The focus of work was extended to data aggregation and ranking of trustworthiness.

Howard A. Blair - Computational Homology, Relativistic Quantum Information and Quantum Programming Languages; Department of Electrical Engineering and Computer Science, Syracuse University

From May 18, 2011 to Aug 19, 2011, the author conducted research on three interrelated projects: (1) computational homology, (2) relativistic quantum information and (3) quantum programming languages. Each of these three projects are a part of on-going work in collaboration with researchers at the Air Force Research Laboratory in Rome, NY in Emerging Computing Technologies Branch of the Division of Advanced Computing Architectures. These projects constitute continuation of work done at AFRL/RL beginning in Summer, 2010, at Syracuse University during the 2010-2011 academic year, at AFRL/RL during Summer, 2011 and will continue at Syracuse University during the academic year 2011-2012 and beyond.

Techniques of computational homology during Summer, 2011, were adapted to detect instabilities in low-dimensional numerical dynamical systems using previously developed techniques of other researchers for this purpose as well as techniques developed in collaboration during both Summer 2010 and Summer 2011 with the author's mentor at AFRL/RL and with other summer faculty and student visitors. The purpose was to detect self-organizing behavior and the signatures of transitions to chaotic behavior in evolving state trajectories of dynamical systems. This led to the preparation and submission of a research proposal by the author to AFRL, Computational Homology for Software Validation. The effectiveness of computational homology in facilitating the detection of these dynamical phenomena was demonstrated with computational experiments. A paper on these experiments will be prepared for submission to a refereed conference proceeding that includes topics on complex systems.

The evolving state trajectory of a spatially separated multipartite quantum dynamical system is subject to the relativistic constraint that information cannot be communicated through the system

faster than light can propagate through the system. There is only limited understanding of the structure of the state trajectories of these systems in the quantum computation community. Quantum cellular automata (QCA) seem particularly well-suited as a model of multipartite quantum dynamical systems. Prior work of some other researchers required a quiescent state to maintain finite support in the global state of these automata. Work performed at Syracuse University during the academic year 2010-2011 by the author and one of his PhD students eliminated the need for the quiescent state and introduced a formal specification logic for constructing mathematically rigorous proofs that quantum dynamical systems probabilistically satisfy specifications defined via pairs of Borel sets in Cantor space defined over the continuum many definite configurations of a QCA. The formal specification logic provides a mathematical semantics for any formalism within which QCA themselves can be programmed. These results were published in a joint paper by the author's PhD student and the author in the SPIE Quantum Information and Computation, IX (April, 2011) conference. During summer 2011, at AFRL/RL the author worked on a not fully resolved problem stemming from the elimination of the quiescent state of a QCA; namely, for only some finite-dimensional unitary operators, their countably infinite tensor powers are unitary. The problem is to characterize the class of such operators. The characterization problem remains not fully resolved and work on it continues at Syracuse University as part of the general research program of the author's research group. The PhD student successfully defended his dissertation on August 25, 2011. Following conversations with participants at the Information Institute's Workshop on Assuring the Cloud (July, 2011), the author applied early work of the category theorist Peter Freyd to construct a general notion of tensor product to apply to both linear and nonlinear dynamical systems during his work in August, resulting in a White Paper submitted to the Air Force Office of Scientific Research on large-scale tractable combining of software systems. Conceptually, this work stemmed from the work on QCA.

Yiran Chen - The Integration And Testing Plans of Neuromorphic Circuitry; Electrical and Computer Engineering Department, University of Pittsburgh

As the 4th fundamental passive circuit element, memristor has recently received increasing attentions since the first real device was reported by HP Lab in 2008. A memristor can record the historic profile of the voltage/current through itself and store the corresponding state permanently. The combined memory and learning capabilities of memristors create great potentials in various system designs, for instance, neuromorphic computing platforms. However, before a very large scale circuit can be implemented, there are many fundamental technical obstacles need to be overcome.

The objective of this project in 2011 summer VFRP was to develop a memristor integration flow for building memristor devices atop synapse circuits. Our proposed research include the following tasks: (1) developing the fabrication and the integration flows of thin film memristive devices atop conventional CMOS process; (2) designing the E-test design modules for CMOS+ memristor circuitry for process and device debugging and circuit design test; and 3) studying the chip testing plan at E-test level, probe pad level and package level. The proposed techniques will be used to integrate the thin film memristive devices with the frontend CMOS circuit of the synapse circuitry designed by other team members, and build the necessary backend metal interconnections.

Baek-Young Choi - Large File Transfer Architecture as a Cloud Service; Department of Computer Science Electrical Engineering, University of Missouri, Kansas City

Bandwidth intensive large file transfer applications such as remote site backup, mirroring and video-over-IP are experiencing momentous popularity. However, their performance does not adequately keep up with the demand. As an Air Force Summer Faculty Fellow, in collaboration with Dr. Keesook Han, Prof. Sejun Song and Prof. Kaiqi Xiong, we have developed a scheme to enhance the performance of large file transfer using efficient file transfer methods in cloud service architecture.

A. Ege Engin - High-Frequency Signal Propagation Through Silicon Medium with TSVS; Department of Electrical and Computer Engineering, San Diego State University

Performance improvement of electronic systems based on CMOS scaling has hit interconnect delay and power consumption barriers in the last decade. Recently emerging 3D ICs eliminate both the power and interconnect barriers. The major new components in 3D ICs are the vertical interconnections called through-silicon vias (TSV).

In this project, we developed analytical formulas to extract an equivalent circuit model for coupled through silicon via (TSV) structures in a 3D integrated circuit. We make use of a multiconductor transmission line approach to model coupled TSV structures. TSVs are embedded in a lossy Silicon medium, hence they behave as metalinsulator-semiconductor (MIS) transmission lines. The developed models can accurately capture the transition between slow-wave and dielectric quasi-TEM modes, which are characteristic for MIS transmission lines, as well as the metal-oxide-semiconductor (MOS) capacitance. The results are validated against 2D quasi-static simulations and 3D full-wave electromagnetic simulations. The derived equivalent circuit models can easily be applied in circuit simulators to analyze crosstalk behavior of TSVs in a 3D integrated system.

Chin-Tser Huang - Router-based Rerouting and Filtering Techniques for Traffic Control in Cloud Computing; Department of Computer Science and Engineering, University of South Carolina

Cloud computing has attracted plenty of attentions and interests because it realizes the long-desired goal of on-demand network access to a scalable shared pool of computing resources, such as servers, storage, applications, platforms, and networks. However, along with cloud computing also come security risks and availability concerns. As an Air Force Summer Faculty, the PI's goal is to enhance the security and performance of cloud computing by developing a router-based technology that when combined with cloud auditing methods will filter malicious traffic early and reroute the excessive legitimate requests to other suitable replicated servers. We had published a paper on a theoretical model to find the best locations for hardware routers in a network to block malicious traffic. We currently focus on developing algorithms to integrate this theoretical model with cloud auditing techniques. In the future work, we will continue the collaboration between University of South Carolina (USC) and the AFRL to design a reliable theoretical model for router-based filtering and rerouting in cloud computing, and conduct experiments to verify the effectiveness of the model.

Qingtang Jiang - Block Compressed Sensing and Generalized Variable Overlapped Window Orthonormal Transform; Department. of Math & Computer Science, Univ. of Missouri-St. Louis

This report consists of three main parts. In the first part we study block-oriented compressed sensing (CS). We observe that for sparse signal recovery, the block CS requires more measurements. We also notice that for approximately sparse images in a basis/system domain, the boundary effect appears in the recovered images with the block CS. We propose two methods to remove the boundary effect: few-pixel overlapping/truncation and few-pixel overlapping/averaging/truncation. After studying the performances of these two methods with different pixel-overlap sizes, we show that if blocks are measured by a CS matrix with an overlap of a few pixels, then the pixel-overlapping methods work well.

The second part of the report is about the variable overlapped window orthonormal transform (VOWOT) and its applications to signal sparse representation and the block CS. We study the relation between the errors and overlapped window sizes in VOWOT-based signal sparse representation. We demonstrate that for a signal on certain intervals, we may need to choose different transforms in VOWOT; and hence we generalize the VOWOT with the sine transform to the generalized VOWOT (GVOWOT) with other transforms. We use GVOWOT to remove the boundary effect and the block effect in the images recovered by the block CS. Furthermore, we use GVOWOT for the block CS-based signal sparse representation.

The third part of the report deals with conclusions and future research directions.

Dhireesha Kudithipudi - A Flexible and Reconfigurable Fabric for Hardware Acceleration; Department of Computer Engineering Rochester Institute of Technology, Rochester Institute of Technology

The aim of this project was to design a reconfigurable FlexiMem layer that can dynamically accelerate portions of the computation. In particular, such design will attain speedups that are in tune with the characteristics of the task. Such fabrics will aid on-demand computing and highly computational and data intensive applications. More importantly such reconfigurable fabrics are extremely suitable for nueromorphic computation where each single device can be treated as a reconfigurable synapse. In some instances of data-intensive applications, FlexiMem can serve as a cache.

Vijay Kumar - Object Discovery, Identification and Association; Computer Science, University of Missouri-Kansas City

Tracking process captures the state of an object. The state of an object is defined in terms of its dynamic and static properties such as location, speed, color, temperature, size, etc. The set of dynamic and static properties for tracking very much depends on the agency who wants to track. For example, police needs different set of properties to tracks people than to track a vehicle than the air force. The tracking scenario also affects the selection of parameters. Tracking is done by a system referred to in this paper as “Tracker.” It is a system that consists of a set of input devices such as sensors and a set of algorithms that process the data captured by these input devices. The process of tracking has three distinct steps (a) object discovery, (b) identification of discovered

object, and (c) object introduction to the input devices. In this paper we focus mainly on the object discovery part with a brief discussion on introduction and identification parts. We develops a formal tracking framework (model) called "Discover, Identify, and Introduce Model (DIIM)" for building efficient tracking systems. Our approach is heuristic and uses reasoning leading to learning to develop a knowledge base for object discovery. We also develop a tracker for the Air Force system called N-CET.

Kim Fook Lee - Quantum Key Generation plus Keyed Communication in Quantum Noise for Free-Space Communication; Department of Physics, Michigan Technological University

The goal of this report is to develop a new type of quantum key generation and encryption scheme for ground based free-space communication. We discuss how to combine Keyed Communication in Quantum Noise (KCQ) and fiber based polarization correlated/entangled photon-pair for efficient keys generation and encryption over a long distance. We will engineer a counter propagating scheme, which can serve two purposes; (i) a heralded single photon source for implementing BB84 protocol, and (ii) polarization entangled photon-pair for implementing Ekert's protocol. The generated secret keys will be automatically feed into the KCQ (Alpha-Eta) for secure data communication. We discuss how to implement quantum key generation based on Keyed Ekert's protocol by using polarization-entangled photon-pair. The Keyed Ekert's protocol has a higher success rate key generation than the original Ekert's protocol. We believe that we can obtain 5500 raw keys in one second with four 25 MHz single photon detectors. After private amplification through classical channel, we expect to obtain 2000 seed keys.

Yingbin Liang - Multi-hub Matrix Theory and Their Applications to Wireless MIMO Communications; Department of Electrical Engineering and Computer Science, Syracuse University

This report summarizes the research work Dr. Yingbin Liang conducted at the Information Directorate of the Air Force Research Laboratory at Rome, NY, during June 20 to August 12, 2010. This work was supervised by Dr. Bruce W. Suter at AFRL/RITB. The technical results of the work is summarized as follows. In this work, we investigated a class of matrices, referred to hub matrices, which contain a number of mutually orthogonal columns and the remaining columns of which have their l2 norms larger than the other columns. The remaining columns are also referred to as hub columns. Bounds on eigenvalues of Gram matrices of single-hub matrices have been recently studied and well-understood, and their applications to wireless communications were demonstrated. Our focus in this work was on multi-hub matrices, for which we derived computable upper and lower bounds on the eigenvalues of their Gram matrices. The idea is based on matrix splitting and applications of the Wyel's theorem. We showed that the complexity of computing these bounds is much less than the complexity of computing the exact eigenvalues if the number of hub columns is much less than the dimension of the hub matrix. Our numerical results demonstrated that for hub matrices the derived bounds are very close to the exact eigenvalues, and are much better than some existing bounds on eigenvalues. We also demonstrated applications of our results on multi-hub matrices to some engineering example problems in wireless multiple-input multiple-output (MIMO) communications, including interpreting hub matrices in the context wireless channel modeling,

characterizing bounds on the capacity of MIMO channels, comparing achievable communication rates corresponding to different transmission schemes, and deriving bounds on the outage probability.

Ruixin Niu - System State Estimation with Data Corrupted by False Information Injection; Department of Electrical and Computer Engineering, Virginia Commonwealth University

The problem of system state estimation in the presence of false information is investigated for linear dynamic systems. It is assumed that an adversary compromises the Kalman filter's ability to estimate the system state, by injecting false information into the sensor measurement only once. The impact of the false information on the Kalman filter's estimation performance is analyzed for a general dynamic system. To be concrete, a target tracking system has been used as an example. In such a system, the effect of the false information on the Kalman filter is proved theoretically to be diminishing over time, even when the Kalman filter is unaware of the false information attack.

Kannappan Palaniappan - Multicore Energy Efficient Architectures and Algorithms for High Performance Video Analysis; Department. of Computer Science, University of Missouri

The parallel video processing algorithms for the IBM Cell/B.E. architecture developed for AFRL includes flux tensor-based motion detection using spatiotemporal derivative and integral filters, integral histogram based feature extraction and a number of additional modules to facilitate tracking such as morphological blob processing, connected component labeling, and blob statistics. This report emphasizes the first two items in the following list of major tasks that were completed:

1. Completion of architecture specific energy efficiency experiments on the parallel flux tensor analysis for moving object detection for presentation at the International Information Fusion 2011 conference in Chicago. Ported implementation to the 16 core IBM QS22 blade server architecture.

2. Reviewed content-based image and video retrieval algorithms, parallelization of image operators using the integral histogram, feature extraction and matching algorithms in the context of video activity understanding for collaboration with Oxford University and Barcelona Supercomputing Center in Spain. Visited Prof. Andrew Zissermans Lab at Oxford University to discuss collaboration with EOARD.

3. Collaborated with Kitware at their facilities to integrate the Matlab-based wide area motion imagery tracking algorithms developed at the University of Missouri with the C++ based image registration, track initialization, and track validation modules developed at Kitware for CETE. Added track termination criteria to reduce the number false alarms, explicit modeling of turns and improved robustness.

4. Explored GPU based versions of the video processing algorithms to study performance and power efficiency tradeoffs for embedded processing. Evaluated techniques such as StarSs from the Barcelona Supercomputing Center to map the video processing algorithms onto a cluster environment using a combination of fine scale and intermediate scale parallelization.

Joon S. Park - A Study for Effective Cloud-Auditing Strategies; Advanced Studies in Information Security Management, Syracuse University

Therefore, as the first step towards satisfying the requirements, through the VFRP 2011 tenure (05/09/2011 – 07/29/2011) I have surveyed the currently available resources that are related to cloud-auditing services, including network monitoring tools, research literatures, standards, and other technical reports, with the research team formed at AFRL. The team consists of Dr. Keesook Han (Advisor, AFRL), Dr. Joon Park (VFRP Faculty, Syracuse University), Edward Spetka (Undergraduate Student, State University of New York Institute of Technology), and Jerry Backer (Graduate Student, New York University). By analyzing the trade-offs of various methods and tools in the area, we have identified the deficiencies in the current approaches and found possible strategies to enhance the current approaches for more effective cloud auditing. We have also extended *Wireshark*, one of the most popular network packet analyzers, by adding a cloud-auditing module, which can be used as a skeleton for future implementation. The findings of this research will be served as a foundation for further research in the area. Based on the survey outcomes, we have provided an oral presentation (20 min.) and a poster [31] at the Workshop on Assuring the Cloud, Griffiss Institute, Rome, NY on July 11, 2011. For further dissemination of the research outcomes, an article, entitled "Cloud Auditing Survey & Advanced Access Control for Assured Clouds [32]," will be submitted to the IEEE International Conference on Cloud Computing Technology and Science (due date: August 21, 2011).

Jing Peng - Experiments with ShareBoost and Randomized ShareBoost; Computer Science Department, Montclair State University

Algorithms combining multi-view information are known to exponentially quicken classification, and have been applied to many fields. However, they lack the ability to mine most discriminant information sources (or data types) for making predictions. We have developed a novel algorithm based on boosting to address these problems. The algorithm builds base classifiers independently from each data type (view) and uses a single re-sampling distribution for all views at each boosting round. This distribution is determined by the view whose training error is minimal. This shared sampling mechanism restricts noise to individual views, thereby reducing sensitivity to noise. We have also established its performance guarantees. In this report, we provide more detailed experimental studies that show its performance with both Naive Bayes and decision trees as base classifiers against noise and competing techniques.

Alfredo Perez-Davila - Impact of Multi-Core Processors on Software; Science and Computer Engineering School, University of Houston – Clear Lake

This report includes the findings of the research performed during the author's participation in the VFRP during the summer 2011 at the Air Force Research Laboratory in Rome NY. The work concentrated in identifying the tools and facilities available for software developers to produce new software applications and/or retrofit existing applications targeted to multi-core platforms. The report describes the motivation for the research, how the research was divided in four areas: Extensions to C/C++; Java Platform, .NET Platform and novel Architectures like those available in advanced graphics cards with hundreds of GPUs (although this last area was not studied in as much detail as the first three). Initially, some general considerations are described which limit the amount of speedup that can be achieved when parallelizing an application, due to the fact that only a fraction of the code will be able to run in parallel. For every application there is always some part which is inherently sequential and therefore cannot run in parallel regardless of the number of cores that are available. For each of the specified areas, an effort was made to identify the facilities available in each of the environments to tackle parallel software development, both from the task parallelization as well as from the data parallelization points of view. It was found that the extensions to C/C++, provided facilities for data and task parallelization both within the Intel Thread Building Blocks (now part of Intel Parallel Studio 2011) as well as through the use of OpenMP. Likewise, .NET and its Parallel Extensions provide similar level of flexibility with facilities for data and task parallelization while the Java environment concentrated on task parallelization and did not seem to provide mechanisms for data parallelization like C/C++ or .NET. The importance of mature tools that can be used to identify the sections of code that can lead to performance improvements through parallelization cannot be over emphasized and in this regard, both C/C++ as well as .NET seem to have a slight edge with the well supported and widely used OpenMP, the Intel Parallel Studio 2011 and Visual Studio 2010 support for Parallel Extensions. Similarly debugging and automatic parallelization tools are available in such environments and can facilitate the developer's job considerably. Finally, some suggestions for future work are presented.

Sachin Shetty - Massive Cloud Auditing Using Data Mining on Hadoop; Department of Electrical and Computer Engineering, Tennessee State University

This report describes our researches in the 2011 Summer Visiting Faculty Research Program from June 2011 to August 2011. Cloud computing allows users to remotely store their data into the cloud and provides on-demand applications and services from a shared pool of configurable computing resources. However, this capability makes evaluation of availability and security of data a very challenging task. Thus, enabling cloud auditing is of critical importance so that users can resort to an external audit party to check the availability and security of outsourced data when needed. The goal of this project is to design and evaluate a system for information exploitation of massive cloud audit logs, which can scale gracefully with increasing number of log traffic. The system development will comprise of three interrelated phases: Traffic Characterization, Online Querying and Distributed Storage and Distributed Incremental Data Mining. The system will provide data mining and analysis on massive cloud data by enhancing data collection, storage and processing capabilities of a open source distributed computing software, Hadoop,

Sejun Song - Clouds for Providing Large File transfer as a Service (FssS); The Dwight Look College of Engineering, Texas A&M University

Large file transfer applications in both traditional data center to data center and cloud computing are experiencing momentous popularity. Despite various available WAN optimization tools and protocol enhancements, the network and system performance of large file transfer does not adequately keep up with the demand. We observe that the problem of poor file transfer performance can be improved significantly via not only network protocols but also an efficient file transfer architecture. This paper proposes a cloud computing architecture for providing file transfer as a service (FaaS) that orchestrate the large file transfer with other available network and system resources in well planned and scheduled manner.

Narayanan Subramanian - Re-Engineering Trustworthy Embedded Systems Using the NFR Approach; Department of Computer Science, The University of Texas at Tyler

Legacy systems are extensively used in the Air Force as well as other military and industrial establishments. Several of these systems were built fifty or more years ago and they are still in operation. Also, many of these systems are of the embedded variety where the software and hardware are closely tied together for a specific purpose. However, in order to re-engineer these systems so that they may be employed on newer platforms, we need to understand the objectives of these systems, namely, their requirements and designs, so that we may modify them to suit modern needs. Modern needs include those of trustworthiness, security, and reliability. This summer our research focused on applying the NFR Approach to re-engineer trustworthy embedded systems. This report summarizes the results of applying the NFR Approach to a test system at AFRL and lessons learnt from that experience.

James M. Vaccaro - Dynamic Planning in a Real-Time Multi-Player Strategy Game; University of San Diego

In this project and described in this report, we examine the strategy game StarCraft and attempt to design, build, and test a prototype dynamic planning tool, which will be used as an autonomous player of the game. The project was a five-month effort at AFRL Rome Research Site and achieved several goals in attempting this challenge. The overall main goal was to produce a player that can learn from playing the game without human assistance, embedded expertise or examining human players' actions. The plan was to develop a player that learned from playing against variations of itself to improve on its own behavior. This task proved daunting for a five-month period, but many aspects of this goal were achieved, and with some additional effort, this main goal is well within sight. Given the complexity of StarCraft and short duration of this project, most of the project focused on the development of plan-generation within the game of StarCraft and the remaining time was spent on plan-execution and assessment implementations. Much still can be gained from this effort, because it supplies a fundamental dynamic planning baseline from which to learn strategies. In the near future, plan-generation, execution and assessment will work together autonomously to learn game playing strategies without human supervision. The ultimate goal is not to build the greatest StarCraft player, but in learning a better StarCraft player, we can gain insight into the usefulness of this architecture and to what learning strategies work for such complex environments. In addition, work on the

dynamic planning architecture produced several results. These results are in six main areas: (1) the plan-generation function was able to produce all unique aspects of the Space Construction Vehicle (SCV) behavior, (2) plan-generation, execution and assessment code was implemented and debugged, (3) in all three phases of planning all the fundamental features of StarCraft are tracked on the fly, (4) plans and unexpected outcomes were generated in a textual format, and (5) plan-generation, execution and assessment all work well independently, can exchange global variables and a visual representation of this dynamical planning system was achieve and demonstrated.

Kaiqi Xiong - An Approach for Reliable and Parallel Large File Transfers in Cloud Computing; Department of Networking and Security, Rochester Institute of Technology

Cloud computing significantly benefits to users and organizations nowadays. Bulk data transfers among cloud users and providers have dramatically increased for the past few years due to the distributed locations of cloud users, services, and resources such as remote cloud data storages. Cloud provider collaborations at national and international levels will further require that a bulk data should be efficiently accessed among a distributed community of cloud users. Such data-intensive applications have evolved in cloud computing, which requires a large file transfer among cloud users, cloud providers, and between them. However, there is a bottleneck in the network connections to and from cloud providers in Wide Area Networks (WANs) for bulk data transfer applications. Thus, a new large file transfer mechanism is urgently desirable for cloud computing. Such a mechanism should be easy deployment and Transmission Control Protocol (TCP) friendliness as well as should allow fast data transfers and should ensure fairness, which is a major challenge in the design. Great efforts have been made to conquer ineffective TCP for the past decade. Among them include Tsunami, SABUL, UDT, RBUDP, FOBS, FRTP (based on SABUL), and Hurricane (based on UDT). However, existing protocols are far from prefect. They are not applicable to parallel processing that not only plays a key in security auditing but also is required in MapReduce service jobs. More importantly, existing protocols such as UDT are only applicable to high speed WANs, which is not a case in most of today's networks. In this project, application-layer end-to-end approaches are developed for reliable and parallel large file transfers in cloud computing. They are UDP-based end-to-end connection-oriented data transport mechanisms for reliably transferring a large size file in a parallel manner. The goals of this research are to first develop and design an approach for large file transfers, and then to evaluate them analytically and experimentally. This report gives a summary of the progress of this research with our future work.

2.2. 2012 Summer Faculty

Bharat Bhargava - Security Properties of Managed Information Object/Active Bundle; Departments of Computer Sciences and Electrical & Computer Engineering, Purdue University

Common approaches for protecting disseminated data (such as Digital Rights Management solutions) against privacy violations use a client application at the host receiving the disseminated data to enforce the privacy policies associated with the data. An alternative approach for protecting disseminated data is to bundle together the data, metadata (policies), and a mechanism that enforces the policies included in the metadata, into a Managed information object (MIO) or active bundle (AB). The common approaches trust the client application to enforce the privacy policies associated to the data. The MIO/AB approach trusts the client host to execute the mechanism that enforces the associated policies. This paper discusses the MIO/AB approach and shows that bundling data with metadata and a policy enforcement mechanism provides enhanced security and reduces the risk of privacy violations for disseminated data. In this paper we extend the MIO to AB, describe the enhanced security features and identify threats to enforcing privacy policies of disseminated data using the attack tree technique. We outline plans for further research and propose multiple methods for reducing the risks of privacy violations.

Howard A. Blair - Geometry of Quantum Entanglement; Department of Electrical Engineering and Computer Science, Syracuse University

The space of (unnormalized) separable states of a quantum system is well-known as a hyperbolic hypersurface, called here the *separation hypersurface* , within the exponentially high dimensional linear space of all (unnormalized) quantum states of a multipartite quantum system. A vector will be on the separation hypersurface if, and only if, the basis-dependent coefficients of the unnormalized separable vector satisfy a tight algebraic constraint the satisfaction of which can be tested in time asymptotically proportional to $d2$, where d is the number of components of the multipartite quantum system. The algebraic constraint entails a closed formformula for a parametric characterization of the entire separation hypersurface of both unnormalized and normalized vectors, the latter being the quantum state factors of separable quantumstates. There are $d¡1$ parameters in the characterization, and the closed form characterization can be obtained in time asymptotically proportional to d. In the case of a separable quantum state of a multipartite quantum system the state of a component of the system can be calculated in worst case in time asymptotically proportional to cd, where c is the dimension of the component. If all components of the system have approximately the same dimension, the time complexity of calculating a component state as a function of the parameters is asymptotically proportional to the time required to sort all of the components.

Marina Blanton - Security Protection of Data and Computation Placed on the Cloud by Android Clients; Department of Computer Science and Engineering, University of Notre Dame

Weak clients such as smartphones are ideally positioned to take advantage of now ubiquitous cloud computing and storage services. Cloud service providers, however, are often third parties that cannot be trusted with clients' proprietary or sensitive information, which is of particular issue for government or military agents. For that reason, it becomes necessary to develop mechanisms for properly protecting the data placed on the cloud by the client or used by the cloud in client-provided computation. This research explores the feasibility of such techniques for Android-based clients.

Yiran Chen - Electrical & Computer Engineering Department, University of Pittsburgh

No report required.

Baek-Young Choi - Cooperative and Opportunistic Mobile Cloud for Energy Efficient Positioning; Department of Computer Science Electrical Engineering, University of Missouri - Kansas City

The fast growing popularity of smartphones and tablets enables us the use of various intelligent mobile applications. As many of those applications require position information, a smart mobile device provides positioning methods such as GPS, WiFi, or Cell-ID based positioning services. However, those positioning methods have different characteristics of energy-efficiency, accuracy, and service availability. In this report, we present an Energy-Efficient Cooperative and Opportunistic Positioning System (ECOPS) for heterogeneous mobile devices. ECOPS facilitates mobile devices with estimated locations using WiFi in cooperation with a few available GPS broadcasting devices, in order to achieve high energy efficiency and accuracy within available budget constraints. ECOPS estimates the location using heterogeneous positioning services and the combination methods including a received signal strength indicator, 2D trilateration, and available power measurement of mobile devices. The evaluation shows that ECOPS significantly reduces energy consumption and achieves the good accuracy of a location.

Yujian Fu - Reconfiguration of Autonomous Robotics Systems; Department of Electrical Engineering & Computer Science , Alabama A&M University

Autonomous robotics systems (ARSs) consist of multiple heterogeneous objects and intelligent inferences that are expected to take appropriate actions even in unforeseen circumstances. Extensive application of ARSs are performed in an extreme environment where human interaction or remote human control is difficult or not even technically feasible. Thus, dynamic reconfiguration of ARSs is a key enabling technology and plays a major role in the future cyber-enabled battle field. To ensure the correct behaviors during reconfiguration, it is highly desirable to have a formal modeling technique for the ARSs so that we can specify the features of such a system in an appropriate way and are able to analyze and verify them by using formal semantics of the modeling approach. Conventional modeling methods like classical Petri nets are restricted to model structural and immutable topologies. Graph transformation systems, in contrast, are

dynamic in their structure but lack a notion of behavior. This summer's research work, focused on the development of a formal approach to the specification and verification of reconfigurability of ARSs. Two typical problems with the ARSs were identified and studied in the summer research work. The first problem, addressed how to formally represent the ARSs and describe the reconfigurable behavior precisely so that the ARSs can adapt to the new changes. The second problem, focused on how to analyze and verify the formal model of the reconfiguration and ensure the correctness of the system during reconfiguration. A case study was developed for application of the approach to a humanoid robot.

Edwin E. Hach, III - Quantum Mechanical Input/Output Analysis of Networks of Directionally Coupled Waveguides and Ring Resonators; Department of Physics, Rochester Institute of Technology

We present a quantum optical analysis of waveguides directionally coupled to ring resonators, an architecture realizable using silicon nanophotonics. Specifically, we envision devices based upon scalable networks of these linear optical elements and operated in a continuous wave (cw) mode. The innate scalability of the silicon platform allows for the possibility of "on-chip" quantum computation and information processing. In this report, we develop a comprehensive method for analyzing the quantum mechanical output of such a network for an arbitrary input state of the quantized, traveling electromagnetic field. Having developed the method, we lay out a general strategy for device design and we present a few results that indicate the promising potential these networks hold for scalable, Linear Optical Quantum Computing and Quantum Information Processing (LOQC/QIP). In developing the theoretical description presented here, we propose a simple model for losses in a ring resonator and we discuss robust on-chip realizations of the Hong-Ou-Mandel Effect. We expect that the results described here will lead to non-trivial, experimentally realizable designs for gates required by LOQC/QIP.

Wei-Da Hao - Semantic Modeling for Cloud Computing and Its Auditing; Electrical Engineering and Computer Science Department, Texas A&M University-Kingsville

We see that opportunities exist to use semantic modeling for cloud computing to improve interoperability and portability issues in current cloud environment. But, in addition to the security and privacy concerns for current cloud, cloud computing with semantic modeling faces even stronger barrier to entry. In this diverse and heterogeneous cloud landscape, we must overcome many challenges to assure the cloud. This report aims to provide the contemporary knowledge of what is cloud computing with semantic modeling and how to evaluate its services. This report explores: semantic cloud, reference architecture for semantically interoperable and portable clouds, model and mechanism of high performance auditing on semantically interoperable and portable clouds. The context in this report should be instrumental to the end users, IT professionals and auditors for a proper audit.

Chin-Tser Huang - Applying Cloud Auditing Techniques to Automate Analysis of Client-Server Interaction in Cloud Computing; Department of Computer Science and Engineering, University of South Carolina

Cloud computing has attracted plenty of attentions and interests because it realizes the long-desired goal of on-demand network access to a scalable shared pool of computing resources, such as servers, storage, applications, platforms, and networks. However, along with cloud computing also come availability and reliability concerns. As an Air Force Summer Faculty Fellow, the PI's goal is to enhance the reliability and performance of cloud computing by applying cloud auditing techniques to automate the analysis of server-client interactions to ensure high performance of clouds. We had published a paper on a theoretical model which models the interaction between server duties and client obligations as interaction strings, and designed an accountability analysis architecture to monitor and analyze the interaction strings. We currently focus on developing a prototype of cookie-based accountability analysis engine to integrate with cloud auditing techniques. Along with my summer intern students, we have also developed apps for Android cookie monitoring and Android packet capturing. In the future work, we will continue the collaboration between University of South Carolina (USC) and the AFRL to complete the implementation of a cookie-based accountability analysis approach, and write papers to publish our extended theoretical model and experimental results.

Robert J. Irwin - Computational Homology; Department of Electrical Engineering and Computer Science, Syracuse University

The author's work this summer at AFRL/RI has been a contribution to the longer-term Computational Homology for Software Validation project currently underway under PI Howard A. Blair. To date, investigation has been ongoing of the dynamics, detectible by computational homology, of low-dimensional numerical dynamical systems using previously developed techniques of other researchers. Working with Howard Blair, Justin Bush and AFRL/RI mentor Paul Alsing, I established software tools for computing algebraic topological invariants of Morse decompositions of Morse sets associated with dynamical systems. In particular, Conley indices were installed on AFRL systems and computational experiments investigating dynamical systems involving non-numerical datatypes begun.

Lifeng Lai - Simultaneous Multiple-Key Generation For Multiple Terminals In Smart Grid; Department of Systems Engineering, University of Arkansas, Little Rock

The problem of simultaneously establishing multiple keys, one for each user in a set of users with the controller, is considered. This scenario arises when there are multiple sensors in the smart grid that want to communicate securely with the controller. For the case of two users, we provide a simple scheme whose performance matches partially with an outer bound developed in the paper. Under certain conditions, this scheme achieves the full capacity region. For the general case of multiple users, we develop a scheme that achieves the sum capacity. We also extend the study to the scenario in which there are several dedicated helpers whose sole purpose is to assist the key generation process for other users. We develop a simple achievable scheme and derive an upper bound for the general case.

Seung-Jong Park - Performance Evaluation of Assured Cloud Computing Centers over Ultra-High Speed Networks Science Department, Louisiana State University

As cloud computing has evolved to provide on-demand virtual services and process unprecedented amount of data, many different kinds of cloud computing clusters have been deployed and operated for mission-critical military applications as well as public applications. In case of emergency, it is critical to federate and drive multiple heterogeneous cloud computing clusters which have been operated by different federal agencies and research institutes. To accomplish time critical missions and succeed a goal, it is necessary to configure software and systems including Hadoop, cloud management software, virtualization software, and operating systems based on the multiple cloud environment and high speed networks. Then PI will evaluate the performance of cloud computing frameworks deployed at multiple clusters which are connected over long distance high speed networking environments. The results of performance evaluation and analysis can be used to improve the performance of Hadoop and cloud computing infrastructures over ultra-high speed networks. The proposed work will help not only mission-critical military applications but also future public cloud applications to increase overall performance of assured cloud computing.

Jing Peng - Combining Multiple Representations for Classification Using Chernoff Distance; Computer Science Department, Montclair State University

Visual object recognition can be formulated as an object-background classification problem. Since combining representations is known to exponentially quicken classification, often different features are used to create a set of representations for a pixel or target object. Each of the representations generates a probability of that pixel being part of the target object or scene background. For example, an image can be represented by (1) texture features, (2) edge features, and/or (3) shape features. Each of these representations provides a partial view about an object of interest, i.e., revealing a particular aspect of the object. Thus, how to optimally combine these representations to effectively exploit multi-modal information for classification becomes a key issue. We propose a novel technique based on the Chernoff distance for exploiting these heterogeneous features for classification. All representations contribute to classification on their learned confidence scores (weights). As a result of optimally combining multi-modal information or evidence, discriminant object and background information is preserved, while ambiguous information is discarded. We provide experimental results that show its performance against competing techniques.

Kaliappa Ravindran - QoS Auditing for Evaluation of SLA in Cloud-based Distributed Services; Department of Computer Science, City College of CUNY and Graduate Center

Given cloud-based realization of a distributed system *S*, QoS auditing enables risk analysis and accounting of SLA violations under various security threats and resource depletions faced by *S*. The problem of QoS failures and security infringements arises due to the third-party control of cloud resources and components that are used in realizing the application-oriented service exported by *S*. The less-than-100% trust between the various sub-systems of *S* is a major issue that necessitates a probabilistic analysis of the application behavior relative to the SLA negotiated with *S*. In this light, QoS auditing allows reasoning about how good the SLA is

complied by *S* in the face of hostile environment conditions. The paper describes case studies of CDN and replicated web service realized on a cloud.

Hamid Sharif – Covert Channels Study and Modeling; Computer and Electronics Engineering Department, University of Nebraska-Lincoln

A covert channel as defined by the Department of Defense's (DoD) Trusted Computer System Evaluation Criteria (TSEC) is "any communication channel that can be exploited by a process to transfer information in a manner that violates the system's security policy." Covert channels are effective means of information hiding and secret communications in computer networks. This has been discussed in literature as a way of intentionally manipulating and embedding hidden information into some properties of the communication networks in such a way that only specific designated user(s) can detect the hidden information.

The primary goal of this project was to study different forms of covert channels in computer networks to lay a foundation for a broad and comprehensive model for understanding covert channels approaches and abstractly discuss analytical models to outline disruption/detection of covert channels. The plan included different types of covert channels and abstractly representing the operations of different covert channels types.

In the first stage of this project, a comprehensive study of covert channels was conducted in direction of the two main fields of protocol---based and the timing covert channels. The focus was on understanding the techniques and approaches for design of covert channels, so methods for disruption and detection of covert channels could be investigated.

The protocol based covert channels utilizes the protocol headers, unused filed, extensions, and pads to hide information. This includes the ubiquitous use of protocols and file structures combined with loose semantics and unused or marginally significant bits, which can be freely used for covert communication channels.

However, our investigation shows that the usage of TCP/IP, the normal IP ID and TCP ISN numbers actually follow a *fairly predictable distribution*, with the actual pattern tied to the operating system. It is possible to detect changes from the anticipated patterns with a high degree of certainty and plan techniques for prevention of protocol based covert channels.

Timing covert channel was also investigated. Covert timing channels modulate the message into temporal properties of the traffic. Instead of using the contents of packets, these channels convey information through the arrival pattern of packets at the receiver, such as individual inter---packet delays.

Broad analytical models were investigated for timing covert channels to exploit the statistical properties of network traffic for prevention or possible detection of covert timing channels. Additionally, the capacity models for covert timing channels were investigated and are presented in this report.

Lixin Shen - Nesterov's Algorithm Solving Dual Formulation for Compressed Sensing; Department of Mathematics, Syracuse University

In this work, we develop efficient algorithms for solving the compressed sensing problem. We modify the standard $\ell 1$ regularization model for compressed sensing by adding a quadratic term to its objective function so that the objective function of the dual formulation of the modified model is Lipschitz continuous. In this way, we can apply the well-known Nesterov algorithm to solve the dual formulation and the resulting algorithms have a quadratic convergence. Numerical results presented in this paper show that the proposed algorithms outperform significantly the state-of-the-art algorithm NESTA in accuracy.

Sachin Shetty - IP Geolocation-based Network Traffic Analysis for Massive Cloud Auditing; Department of Electrical and Computer Engineering, Tennessee State University

This report describes our researches in the 2012 Summer Visiting Faculty Research Program from June 2012 to August 2012. Security of user data in the cloud requires adequate protection of cloud computing system and network. Network traffic analysis for cloud auditing is of critical importance so that users can resort to an external audit party to verify the security of the network between user and provider. To satisfy these technology requirements, we develop a machine learning based method for accurate IP geolocation of cloud servers and network devices. The ability to localize Internet hosts is appealing for a range of applications from online advertising to localizing cyber attacks. Recently, measurement-based approaches have been proposed to accurately identify the location of Internet hosts. These approaches typically produce erroneous results due to measurement errors. In this paper, we propose an Enhanced Learning Classifier approach for estimating the geolocation of Internet hosts with increased accuracy. Our approach extends an exisiting machine learning based approach by extracting six features from network measurements and implementing a new landmark selection policy. These enhancements allow us to mitigate problems with measurement errors and reduce average error distance in estimating location of Internet hosts. To demonstrate the accuracy of our approach, we evaluate the performance on network routers using ping measurements from PlanetLab nodes with known geographic placement. Our results demonstrate that our approach improves average accuracy by geolocating internet hosts 100 miles closer to the true geographic location versus prior measurement-based approaches.

Sejun Song – Smartphone Cloud for Distributed Data Processing with Applications to Mobile Security and Monitoring; Telecommunications Engineering, Texas A&M University, College Station

Android Smartphone Cloud (ASC) aims to create a collaboration environment to interface smartphones and cloud servers. Android Smartphones are unable to perform security monitoring tasks due to memory and CPU limitations. The goal of this research is to develop client-side ASC and server-side distributed Hadoop systems to utilize cross-side security monitoring technology for a feasible cloud auditing. We have developed an ASC and cross-side security monitoring technology.

Alex Sprintson - Design, Development, and Performance Evaluation of Mobile Cloud Computing Systems; Department of Electrical and Computer Engineering, Texas A&M University

Research activities have focused on developing the Android Smartphone Cloud platform. In collaboration with other members of the CyberBat team, we have implemented efficient and effective smartphone cloud environment that enables robust distributed data processing, supports diverse reusable applications components and features modular architecture. The proposed solutions have a potential to significantly improve the reliability and robustness of mobile information systems as well as improve the access to information and computational power for solders at the battlefield.

Narayanan Subramanian - Identifying Trustworthiness Deficit in Legacy Systems Using the NFR Approach, Department of Computer Science; University of Texas at Tyler

Trustworthiness is an important emerging requirement for software systems deployed by the U. S. Air Force. Trustworthiness, briefly stated, is the ability of a software system to be safe, secure, and reliable under normal operating environment. However, most software systems have not been developed with trustworthiness in mind. Therefore, software systems in operation have trustworthiness deficit – that is, they lack trustworthiness to some extent. We would like to systematically identify this deficit in trustworthiness in existing systems so that they may be re-engineered with trustworthiness as a priority. The advantages of identifying this deficit include determination of trustworthiness in current systems, exploring environments in which current systems may be (re)used, and prioritizing trustworthiness requirements when these legacy systems are re-engineered. The NFR (non-functional requirements) Approach provides a framework for identifying gaps in trustworthiness in existing systems and recommending mechanisms to overcome this "shortfall" in re-engineered systems. In this project we extended our research in re-engineering using the NFR Approach performed during the summer of 2011 to identify trustworthiness deficit in legacy systems. The NFR Approach can be applied at the requirements and design levels, the earliest phases in the development of a software system, and therefore, we identified trustworthiness deficit at the requirements level, and techniques for reducing this deficit at the design level. The NFR Approach uses structures called the Softgoal Interdependency Graph (SIG) for analyzing softgoals, which are representations for requirements and designs of the software system. For deficit analysis, we identified the overlaps between the SIG capturing the NFRs of the legacy system and the SIG capturing the requirements for the trustworthy system. This overlap analysis led to the development of the Deficit Equation that measures the extent of trustworthiness deficit in the legacy system. For case-study we used the Phoenix system, a middleware system used by the Air Force. Using this equation we estimated the trustworthiness deficit in the Phoenix system to be 89%, which is relatively high. In the next step we identified techniques that will help reduce the deficit using the NFR Approach. We identified at least three design modifications for the legacy Phoenix system that will help improve its trustworthiness. We finally verified and validated our results by obtaining feedback from Phoenix's development engineers on our conclusions. Our study gives high confidence in the suitability of the NFR Approach for trustworthiness deficit analysis for generic software systems. Based on this case-study we also developed a process for applying the NFR Approach for trustworthy deficit identification and deficit mitigation for software systems.

Madjid Tavana - The Stability Model: An Interactive Framework for Measuring Robustness and Resiliency in Military Command and Control Systems; Department of Information Systems and Decision Sciences, La Salle University

The increasing complexity and tight coupling between people and technology in military Command and Control (C2) systems has led to greater vulnerability due to system failure. Although system vulnerabilities cannot be completely eliminated, the accidental or anticipated failures have to be thoroughly understood and guarded. Traditionally, the failure in C2 systems has been studied with resiliency and the concept of self-healing systems represented with reactive models or robustness and the concept of self-protecting systems represented with proactive models. We propose the *stability* model for simultaneous consideration of robustness and resiliency in C2 systems. Robustness and resiliency are measured with multiple criteria (i.e. repair-recovery times and repair-recovery costs). The proposed interactive framework plots the robustness and resiliency measures in a Cartesian coordinate system and derives an overall *stability index* for various states of the C2 system based on the theory of displaced ideals. An ideal state is formed as a composite of the best performance values and a nadir state is formed as a composite of the worst performance values exhibited by the system. Proximity to each of these performance poles is measured with the Euclidean distance. The C2 system should be as close to the ideal state as possible and as far from the nadir state as possible. The stability index is a composite measure of distance from the ideal and nadir states in the C2 system. We present a case study at the Air Force Research Laboratory to demonstrate the applicability of the proposed framework and exhibit the efficacy of the procedures and algorithms.

Dmitry Uskov - Designing Optimal Schemes for Photonic Cluster Sate Generation; Division of Mathematics and Science, Brescia University & Department of Physics and Engineering Physics, Tulane University

Our theoretical research was focused at the problem of photonic cluster-state quantum computation. We suggested a new scheme of cluster state generation for 4, 6 and 8 qubits. By its design the scheme provided the most efficient method of cluster state generation. Finding optimal quantum schemes of generating non-classical photonic states is of crucial importance for the whole field of photonic quantum computation since the only photon-photon entangling operations implementable currently in a lab are measurement-assisted stochastic quantum transformations. There are about 7 competing experimental groups in the world which currently possess enough experience and technology to generate multiqubit cluster states. All of these groups are using the same scheme, designed more than a decade ago when photonic quantum information science was at the state of infancy. Our theoretical results demonstrate that this method is by far not the optimal one. Analyzing quantum efficiency of state generation by efficient numerical optimization algorithms we discovered a new scheme of cluster state generation which boosts the success rate of generation by more than one order of magnitude even for a small eight-qubit cluster. The advantage of our scheme in comparison with traditional scheme grows exponentially fast with the size of cluster. Therefore we expect that all future experiments with photonic clusters will be based on our current results.

Jonathan White - Increasing the Survivability, Reliability, and Utility of Systems in Contested Environments; Department of Engineering and Physics, Harding University

This final report details the work that was performed in the summer of 2012 related to securing, modeling, and increasing the survivability of contested environments. This report details three discrete works that were began this summer. All of the three works will result in publications and this summer was the most productive time of research that I have ever had.

The first work relates to automatically identifying critical data in a database by using historical database logs and making a tree-based data structure that is processed with a novel algorithm to reveal the most critical data. The next stage of this database related work uses this information to deploy a large amount honeytokens throughout the environment, which mimic these critical data items without in fact being critical to the operation of the organization. These honeytokens effectively act like land mines or early warning beacons, discouraging data misuse and enhancing the security of the system.

The second work that was begun is related to securing text messaging systems by also using honeytoken ideas. This model works by populating a mobile device with several thousand highly realistic text messages that serve as decoys. These deceptive texts look like the real thing, and if your cell phone is illicitly accessed, the attacker must sort through all the messages, both real and fake, and they get a much more inchoate view of your communication network and what your digital activities entail. These synthetic texts are downloaded to the device from a webpage and do not incur a per-text charge from the cell company. The clone texts are designed so that they are easily ignored or not even seen by the legitimate user using methods that are described below. Conversely, the doppelgangers are not so easily ignored by an unknowledgeable attacker, creating an asymmetry that improves the survivability of the device under attack.

The third area of work is a method that increases the correctness and usefulness of survivability models that are aimed at increasing the survivability of mobile devices that are deployed in the field. We are researching this important problem because Air Force networks that embrace common off the shelf (COTS) technology must be resilient to both hardware issues caused by the harsh physical environment and also software issues caused by the contested cyber environment. By combining information available from both domains, we arrive at a much clearer picture of the survivability of the device and the model can much more accurately predict when the device might fail (which will be more common as the device is COTS). If the COTS device can be swapped out with a fresh device before complete failure occurs, the ensuing downtime and loss of data can be minimized, making the proposed model very important to DOD needs

Kaiqi Xiong - Service Level Agreement (SLA)-Based Resource Management For High-Performance Cloud Auditing; Department of Networking and Security, Rochester Institute of Technology

This chapter will start with an introduction of Service Level Agreement (SLA) and the Quality of Service (QoS) metrics defined in an SLA. It will give the formal definition of each QoS metrics with a study of their relationships. The discussed QoS metrics include security, performance, and availability. As is noticed, security usually includes identity security and behavior security. This chapter is also concerned with the three most important performance metrics: response time,

throughput, and utilization. It will describe an overview of existing approaches for resource management in various computing systems through an emphasis of cloud computing. Moreover, this chapter will present the SLA-based approaches for resource management in high-performance cloud auditing. That is, this chapter will study trustworthiness, a percentile of response time, and availability in the SLA-based approaches. We will first quantify these metrics and then formulate resource management as a nonlinear optimization subject to SLA requirements that are expressed as the quantifications of these metrics. Finally, this chapter will provide us with a solution of this nonlinear optimization problem and demonstrate its effectiveness through an illustrative example.

Shouhuai Xu - Department of Computer Science, University of Texas at San Antonio

No report required

Tianyu Yang - Efficient Adaptive Techniques For Digital Beamforming And I/Q Equalization In Wireless Receivers; Department of Electrical, Computer, Software and Systems Engineering, Embry-Riddle Aeronautical University

This research project studies efficient adaptive signal processing techniques for two important applications in wireless communications: “image” frequency band interference suppression and digital beamforming. For each application, an adaptive technique is employed at the wireless receiver’s baseband in the digital signal processor. During the adaptation process, time-varying weight update is automatically generated at each iteration to achieve improved interference suppression performance and convergence behavior. Computer simulations are performed in MATLAB to validate the effectiveness of the proposed adaptive techniques. The simulation results confirm that, compared to existing methods, the presented techniques exhibit better interference suppression performance and/or convergence properties under various communication scenarios.

Janusz Zalewski - Modeling and Analysis of Trust Attributes in Software:Threat Modeling for Security Assessment in Cyberphysical Systems; Department of Software Engineering, Florida Gulf Coast University

The work presented in this report is a continuation of two previous phases conducted in 2011: Summer Project titled “Relationships between Safety and Security and Their Implications in Building Trustworthy Systems”, and its follow-up “Modeling Trustworthiness Properties in Critical Embedded Systems and Networks.” The previous work resulted in several recommendations for a more focused study of security modeling, in particular, with respect to computational models using discrete event simulation tools, expanding it to threat modeling. In the current report, threat modeling issues in cyberphysical systems are discussed. First a generic model of a cyberphysical system is outlined, with an attack surface suitable for security analysis, including four types of interfaces (process interface with sensors and actuators, user interface, network communication interface and database interface), as well as disturbances encompassing threats and affecting not only the process but also the controller. Then, a case study of network communication in a road vehicle is presented, with its behavior modeled by a discrete time Markov chain, under the assumption that security violations can cause gradual degradation of

functionality, rather than all-or-nothing type of security breaches. Finally, two ways of numerical assessment of vulnerabilities are presented, to help better estimate probabilities of state changes in a Markov model: one more traditional based on a STRIDE/DREAD approach, and a newer one involving the Common Vulnerability Scoring System (CVSS). Experiments with an example of threat modeling for a cyberphysical system, an automotive Controller Area Network (CAN), are discussed.

Jingyuan Zhang - Synchronized PowerPoint Slide Shows for Large Video Walls; Department of Computer Science, University of Alabama

Nowadays it is not uncommon to have an LCD video wall in a large conference room. An LCD video wall consists of multiple LCD panels tiled together almost seamlessly, and it is usually driven by a single computer. Microsoft PowerPoint is probably the most popular application used on these video walls. However, PowerPoint permits only one slide show that is centered within a video wall. As a result, there is tremendous waste of display real estate and the audiences at the sides do not have a good view of the slide show. This project developed software that extends PowerPoint to allow multiple synchronized slide shows on a video wall. The developed software allows dual simultaneous slide shows as well as one slide show. With the developed software, a slide show can be placed anywhere on the video wall to accommodate the audience and dual slide shows can be run synchronously. The developed software greatly reduces waste of display real estate and allows the audience to see the slide show better.

Martin Q. Zhao - Study of *SITA* System Design and Messaging Mechanisms; Department of Computer Science, Mercer University

SITA is a component-based Situation Awareness (SA) system that

- Takes in sensory data;

- Identifies the current situation;

- Assesses the impact of that situation; and

- Projects “plausible” futures (with threat ratings).

Initiated and tested based on a Cyber security environment, this system was aimed to deal with SA and decision support for all domains of concerns for the Air Force.

With the inclusion of basic event tracking, impact assessment, and future projection functions into SITA 1.0 by the end of 2011, efforts have been carried out to incorporating models that project “plausible” futures into the subsequent SITA versions. Modules that take advisory characteristics (past behavior, capacity/capability, opportunity, etc.) into account are under development.

The goal and objectives of this summer VFRP effort was to start a thorough process of exploring ways to quantify the benefits and effectiveness of including various models into the process of projecting “plausible” futures. In-depth analysis need to be conducted to figure out increase in metrics such as recall and precision when these models are included to the projection process, as well as associated response delays.

3. CONTINUING RESEARCH PROJECTS

3.1. 2011 Faculty Extension Grants

Mainak Chatterjee - Bargaining Framework for Network Co-existence in Unlicensed Spectrum Bands; Department of Electrical Engineering and Computer Science, University of Central Florida

In this project, we address the problem of dynamic channel access by a set of cognitive radio enabled nodes, where each node acting in a selfish manner tries to access and use as many channels as possible, subject to the interference constraints. We model the dynamic channel access problem as a modified Rubinstein-Ståhl bargaining game. In our model, each node (player) negotiates with the other nodes to obtain an agreeable sharing rule of the available channels, such that, no two interfering nodes use the same channel. We solve the bargaining game by finding Subgame Perfect Nash Equilibrium (SPNE) strategies of the game. We consider finite horizon version of the bargaining game and investigate its SPNE strategies. Furthermore, we identify Pareto optimal equilibria of the game for improving spectrum utilization. The bargaining solution ensures that no node is starved of channels

Mainak Chatterjee - Collaborative Jamming and Collaborative Defense in Cognitive Radio Networks; Department of Electrical Engineering and Computer Science, University of Central Florida

Cognitive Radio Network (CRN) is one of the prominent communication technologies that is touted to drive the next generations of digital communications. In this paper, we address the vulnerabilities in such networks and analyze a common form of the Denial-of-Service attack, i.e., collaborative jamming. In particular, we model and analyze the channel availability when different jamming and defending schemes are employed by the attackers and legitimate users. Cooperative defense strategy is proposed to exploit the temporal and spatial diversity for the legitimate secondary users. Illustrative results show how to improve the resiliency in CRN against jamming attacks.

A. Ege Engin - 3D IC Test Vehicle Design for Testing of RF Properties of Through Silicon VIAS; Department of Electrical and Computer Engineering, San Diego State University

This project is an extension of the VFRP project with the title ”High-Frequency Signal Propagation through Silicon Medium with TSVs” that was performed in Summer 2011. The summer project resulted in a new analytical approach to extract an equivalent circuit model for coupled through silicon via (TSV) structures in a 3D IC. We made use of a multiconductor transmission line approach to model coupled TSV structures. The developed models accurately captured the transition between slow-wave and dielectric quasi-TEM modes, which are characteristic for metal-insulator-semiconductor (MIS) transmission lines, as well as the MOS capacitance.

In the extension project, full-wave electromagnetic simulations were done to characterize the scattering parameters of TSV configurations investigated during the summer project. Excellent

match between developed models and fullwave simulations were observed. A measurement and deembedding methodology was developed for TSV test structure design for RF testing. Based on this methodology, it will be possible to characterize the full coupling matrices of a TSV array, by properly deembedding measurements obtained through a calibrated vector network analyzer.

Qingtang Jiang - Adaptive Bases for Compressed Sensing and an Algorithm for Block-Effect Removal; Dept. of Math & CS, Univ. of Missouri-St. Louis

This report summarizes the author's work carried out under the support with the extension grant. This report consists of four main parts. In the first part, we introduce some backgrounds on compressed sensing and address the problems considered in this project. In the second part, we propose the adaptive-basis approach for signal recovery in compressed sensing. In the third part, we provide an algorithm to remove the block-effect which sometimes appears in the recovered image by the block-oriented compressed sensing. In our algorithm we add constraints on the boundary. We show this algorithm can be formulated as the conventional l1-minimization problem. In fourth part of the report, we give the conclusions and provide future research directions.

Ruixin Niu - Dynamic System State Estimation in the Presence of Continuous False Information Injection; Department of Electrical and Computer Engineering, Virginia Commonwealth University

The problem of state estimation in the presence of continuous false information injection is investigated for linear dynamic systems. It is assumed that an adversary compromises the Kalman filter's ability to estimate the system state, by injecting false information into the sensor measurement continuously over time. The impact of the false information on the Kalman filter's estimation performance is analyzed for a general dynamic system. To be concrete, a target tracking system has been used as an example. In such a tracking system, the extra state estimation error caused by repeated false information injection is proved theoretically to reach a finite steady state, whose relationship with the target maneuvering index is investigated as well.

Alfredo Perez-Davila -

Award declined; Award withdrawn

Sachin Shetty - Massive Cloud Auditing using Data Mining on Hadoop; Department of Electrical and Computer Engineering, Tennessee State University

Cloud computing allows users to remotely store their data into the cloud and provides on-demand applications and services from a shared pool of configurable computing resources. However, this capability makes evaluation of availability and security of data a very challenging task. Thus, enabling cloud auditing is of critical importance so that cloud providers can monitor the availability and security of outsourced data in the cloud when needed. In this report, we present the design of the network cloud auditing system which includes secure and reliable geolocation, online querying and anomaly detection services to track the activity of cloud users.

Sejun Song - Router-Initiated Network Outage Management for Multitenant Clouds: Building an OpenFlow-based Test Bed; Telecommunications Engineering Department, Texas A&M University

Existing remote Network Management System (NMS) centric outage management practices are unreliable, inaccurate, and not scalable that cannot be directly used in multitenant clouds. We have proposed a vendor neutral, router embedded, and distributed outage management system which provides scalability, accuracy, reliability, and autonomy on the outage management. In this project, we have created a prototype of the proposed system using an Openflow architecture. We use both NetFPGA and OpenWrt based open source router environments. We have detected and evaluated CPU usage problems under DDoS scenarios

Jian Tang - Survivable Virtual Machine Management in Data Centers; Electrical Engineering & Computer Science Department, Syracuse University

In a virtualized data center, survivability can be enhanced by creating redundant VMs as backup for VMs such that after VM or server failures, affected services can be quickly switched over to backup VMs. To enable flexible and energy-efficient resource management, we propose to use a service-aware approach in which multiple correlated Virtual Machines (VMs) and their backups are grouped together to form a Survivable Virtual Infrastructure (SVI) for a service or a tenant. A fundamental problem in such a system is to determine how to map each SVI to a physical data center network such that operational costs (such as the energy usage cost) are minimized subject to the constraints that each VM's resource requirements are met and bandwidth demands between VMs can be guaranteed before and after failures. This problem can be naturally divided into two sub-problems: VM Placement (VMP) and Virtual Link Mapping (VLM). We present a general optimization framework for this mapping problem. Then we present an efficient algorithm for the VMP subproblem as well as a polynomial-time algorithm that optimally solves the VLM subproblem, which can be used as subroutines in the framework. We also present an effective heuristic algorithm that jointly solves the two subproblems. It has been shown by extensive simulation results based on the real VM data traces collected from the green data center at Syracuse University that compared with the First Fit Descending (FFD) and single shortest path based baseline algorithm, both our VMP+VLM algorithm and joint algorithm significantly reduce the reserved bandwidth, and yield comparable results in terms of the number of active servers.

Jay Urbain - Semi-supervised Relational Learning for Entity, Event, and Relation Discovery; Electrical Engineering and Computer Science Department, Milwaukee School of Engineering

Over the course of the summer, we performed an extensive literature review of state-of the-art methods for entity and relation extraction. We experimented with several techniques which resulted in the development of an experimental search engine framework for performing adhoc *entity-relation* search. Extraction of general entity classes such as people, locations, and organizations is a mature research area. Relation extraction, identification of fine-grained entities, and performing these operations adhoc are open research problems.

In our proposed framework, the user defines *entity classes* (e.g., *terrorist*), representative *entity seed instances* (e.g., *KSM, Sayef, etc*.) for each class, and *entity-relations* consisting of two entity classes (e.g., *terrorist* and *financial organization*). To learn an *entity-relation pattern*, the underlying search engine retrieves candidate sentences containing instances of *entity seeds* for each *entity class* in an *entity-relation*. From the retrieved result set, the user identifies which sentences are relevant, i.e., exhibit the *entity-relation* to learn, and then submits these selections to the search engine. The search engine attempts to learn patterns from the sentences that are most likely to identify the existence of the *entity-relation*. Once an *entity-relation pattern* is learned, the user can search for entity instances that participate in the same *entity-relation*. This process can continue in an iterative fashion. If the user discovers new instances of entities or candidate sentences, they can be "added" to reinforce the efficacy of the learned model. If specific *entity instances* or learned *entity-relation patterns* are ineffective, they can be removed.

Our approach for learning *entity-relation patterns* involves the extraction and mining relational dependency sequences between entity instances. Preliminary results achieved on a small in-house collection of intelligence reports looks promising. Our goal is to develop user-driven contextual models of entities and their relational dependencies, and a search system based on this model that allows users to not only search for known entities and relations, but discover new relations from known entities, and discover new entities from known relations.

Michael C. Wicks - Layered Networking Software Defined Radio Sensing Experiment; University of Dayton

In order to fully implement and exploit Compressive Sensing in Distributed and Layered Sensing systems, a secure and reliable network for connectivity is essential. As Commercial Off-The-Shelf technology already dominates the DOD networking infrastructure, and is replacing custom networking technology in fielded weapons, a futuristic "Layered Network" specifically for military applications becomes attractive. A Layered Networking Architecture for Distributed and Layered Sensing is considered in this study, emphasizing homogeneous RF sensors, enabled by a Cognitive SWDR for Layered Networking – a technology that may eventually overlay a commercial communications network, thus adding robustness, a degree of enhanced security, and graceful degradation during commercial network failure. Another aspect of this initial systems level study is the efficient implementation of algorithms and architectures to accomplish the aforementioned goals of secured and reliable connectivity for Distributed and Layered Sensing in an integrated fashion. As such, this new Layered Network could ultimately be embedded in individual compressive-sensing nodes, in parallel with electronics for conventional networking. More generally, this Layered Networking concept could be developed as the infrastructure interfacing custom sensors to the cloud-computing network which is rapidly emerging as a commercially viable alternative to classically defined data storage and computing platforms.

An important aspect of this investigation was the planning for demonstration of Layered Networking for Compressive Sensing. This could be accomplished at the Stockbridge Test Site using the residual capability from RF Tomography experiments recently concluded by AFRL Sensors Directorate personnel. Using several towers already instrumented with antennas and RF cabling, the basic infrastructure is in place for experiments which could permit validation of new techniques in Compressive Sensing, and permits the incremental incorporation of Layered

Networking in parallel with existing commercial networking technology. The remaining towers at Stockbridge could serve to host test targets and instrumentation for "calibration of the test scene." Alternatively, experiments could be conducted at the newly constructed Outdoor Range experimental facility at WPAFB in Ohio. This initial study provides concepts for demonstrating novel techniques in Cognitive SWDR based Layered Networking in support of Compressive Sensing, potentially providing secure and reliable connectivity between and among individual sensor nodes (a network which parallels and compliments commercially available networking electronics, and demonstrates new and novel concepts prior to fielding this technology).

Kaiqi Xiong - Resource Allocation for Sla-Guaranteed Reliable and Parallel Large File Transfer in Cloud Computing; Department of Networking and Security, Rochester Institute of Technology

Cloud computing has recently played one of the most roles in today's business. Bulk data transfers among cloud users and providers have dramatically increased for the past few years due to the distributed locations of cloud users, services, and resources such as remote cloud data storages. Cloud provider collaborations at national and international levels will further require that a bulk data should be efficiently accessed among a distributed community of cloud users. Such data-intensive applications have evolved in cloud computing, which requires a large file transfer among cloud users, cloud providers, and between them. Great efforts have been made to conquer ineffective TCP for the past decade. Among them are a variety of techniques such as Tsunami, SABUL, UDT, RBUDP, FOBS, FRTP (based on SABUL), and Hurricane (based on UDT). But, existing protocols are not applicable to parallel processing. However, parallel processing not only has played a key in security auditing but also is required in MapReduce service jobs. More importantly, existing protocols such as UDT are only applicable to high speed WANs, which is not a case in most of today's networks. In the previous research, application-layer end-to-end approaches are developed for reliable and parallel large file transfers in cloud computing. They are UDP-based end-to-end connection-oriented data transport mechanisms for reliably transferring a large size file in a parallel manner in which sufficient cloud resources need to be allocated to meet the Quality of Services (QoS) requirements of cloud users defined in a Service Level of Agreement (SLA). The SLA is a contract agreed between cloud users and a cloud provider in the bulk data transfers. The goals of this research are to first characterize the end-to-end QoS performance metrics of a user and provide their calculation, and then develop the optimal solutions for mapping virtual resources to meet the need of cloud service workloads for ensuring SLA guarantees that will be applicable to use in real-world applications. This report gives a summary of the research findings with our future work

Janusz Zalewski - Modeling Trustworthiness Properties in Critical Embedded Systems and Networks; Department of Computer Science, Florida Gulf Coast University

This project, as an extension of the Summer 2011 AFRL Faculty Fellowship, studied additional issues related to modeling trustworthiness properties in embedded systems and networks. It continued the summer project in the following aspects:

1) Analyzing security and safety in a broader context of system trustworthiness, including reliability.

2) Building a specific model of a trustworthy architecture, suitable for focusing on the analysis of trustworthiness of embedded systems and networks.

3) Involving a Case Study suitable for conducting security analysis under unpredictable conditions.

4) Building and analyzing models of trustworthiness with the use of automatic modeling tools.

With respect to (1), an extensive literature study was conducted, focused on aspects of assessing security in a broader context of safety and dependability. As a result, around a hundred literature entries published over the last decade were analyzed with respect to security assessment. Together with the literature studied during the summer project, it forms a good basis for a survey paper to submit, for example, to the ACM Computing Surveys.

Regarding (2), following a thorough literature study, involving over fifty entries, extensions to theoretical, experimental, and computational models of security assessment were suggested, enhancing those developed during the summer project. A related paper was presented at the CSIIRW 2011 - 7th Annual Cyber Security and Information Intelligence Workshop. Another paper was accepted for presentation at the Systems and Software Technology Conference, in Salt Lake City, April 23-26, 2012.

With respect to (3), a generic embedded controller model to interface with a controlled process, was found to be compatible with the distributed control system models used in industry. In particular, the network interface security aspects of the model were proposed for analysis with the use of SCADA, as an experimental platform. Also in this view, a literature review was conducted to analyze approaches to assess operational security in distributed computer control systems.

Finally, based on the results of the model selection, a number of security tools were analyzed, and a choice was made to use four of them in the case study. With the use of Wireshark and Metasploit, a study conducted on the experimental SCADA platform available at the Florida Gulf Coast University's lab. In a view of these results, the following recommendations can be made for future work:

Expand the theoretical models of security assessment based on reasoning about uncertainty, with applications of the rough sets enhanced with the use of Bayesian belief networks.

Deepen the experimental security assessment with the use of industry strength monitoring and penetration tools for a practical platform (not only virtual), such as SCADA.

Continue investigation of security assessment with computational models using discrete event simulation tools, perhaps expanding it to threat modeling.

3.2. 2012 Faculty Extension Grants

Bharat Bhargava - Scalable, Robust, and Secure Information Management in Cloud; Computer Sciences and Electrical & Computer Engineering, Purdue University

Common approaches for secure data sharing and protecting disseminated data in Cloud against privacy violations require an active and trusted entity to enforce the privacy policies associated with the data. An alternative approach for protecting disseminated data is to use a secure Managed Information Object (MIO) or an Active Bundle (AB) that bundles together the data, metadata (policies), and a protection mechanism that protects the bundle and enforces the policies. The common approaches trust the active and trusted entity to enforce the privacy policies associated with the data. The MIO/AB approach trusts the data recipient to let Active Bundle execute and enforce the associated policies. This report focuses on the MIO/AB approach and shows that bundling data with metadata and a policy enforcement mechanism provides enhanced security and reduces the risk of privacy violations for disseminated data in a scalable Cloud environment. We extend the basic MIO to enhanced AB, describe the enhanced security features and identify threats to enforcing privacy policies. We propose multiple methods for reducing the risks of privacy violations.

Howard A. Blair– Geometry of Quantum Entanglement; Department of Electrical Engineering and Computer Science , Syracuse University

The space of (unnormalized) separable pure states of a quantum system is well-known as a hyperbolic hypersurface, called here the *separation hypersurface*, within the exponentially high dimensional linear space of all (unnormalized) quantum states of a multipartite quantum system. A state of a multipartite quantum system with n components can be viewed as a n-dimensional hypermatrix. A vector will be on the separation hypersurface if, and only if, the basis-dependent coefficients of the unnormalized separable vector satisfy a tight algebraic constraint the satisfaction of which can be tested in time asymptotically proportional to n^2, where n is the number of components of the multipartite quantum system: the determinant of every 2-by-2 2-dimensional submatrix of the hypermatrix is 0. This algebraic constraint entails a closed form formula for a parametric characterization of the entire separation hypersurface of both unnormalized and normalized vectors, the latter being pure quantum states, by completely factoring the separable state. The characterization is dependent on $n-1$ parameters and can be obtained in time asymptotically proportional to n. The hypermatrix also allows factoring of partially separable pure states by aggregating components and yields a means of quantifying entanglement in a pure quantum state that can in turn be used in quantum programs to obtain partial control of the effects on a quantum register due to measurement of some of its qubits. The hypermatrix view of a pure quantum state allows for quantifying entanglement within sub-hypermatrices of the pure state as in the case, for example, of the pure state of a 3-qubit register restricted to a subset of the computational basis such as $\{|000\rangle, |001\rangle, |110\rangle, |111\rangle\}$.

Marina Blanton – A Comprehensive Toolset for General-Purpose Private Computing and Outsourcing; Department of Computer Science and Engineering, University of Notre Dame

The goal of this rather large-scale project is to develop techniques suitable for secure computation in a variety of settings including secure joint computation and secure outsourcing, as well as foster their practical use. The work supported by this extension grant focused on building an initial version of a compiler that takes a general-purpose functionality written in an extension of the C programming language and translates it into secure distributed computation implementation. This report details the design of such a compiler and currently supported functionality.

Mainak Chatterjee – Network Diversity for Survivability of Cyberspace; Department of Electrical Engineering and Computer Science, University of Central Florida

In this project, we attempt to characterize the QoS that secondary users can expect in a cognitive radio network. Using power control as a black-box, we propose a method that can help us evaluate the QoS for any given power vector based on past observations. To that end, we first define a k-dimensional QoS space where each point in that space characterizes the expected QoS. We show how the operating condition of the system maps to a point in the QoS space, the quality of which is given by the corresponding QoS index. To deal with the real-valued QoS space, we use vector quantization to partition the space into finite number of regions each of which is represented by one QoS index. We argue that any operating condition of the system can be mapped to one of the pre-computed QoS indices using a simple look-up in $O(\log n)$ time– thus avoiding any cumbersome computation for QoS evaluation. Using simulations, we illustrate how a 2-dimensional QoS space can be constructed. We choose capacity as the QoS metric and show what the expected capacity would be for a given power vector.

Yiran Chen – Mobile User Classification and Authorization Based on Gesture Usage Recognition; Electrical and Computer Engineering Department New York University of Pittsburgh

Intelligent mobile devices have been widely serving in almost all aspects of everyday life, spanning from communication, web surfing, entertainment, to daily organizer. A large amount of sensitive and private information is stored on the mobile device, leading to severe data security concern. In this work, we propose a novel mobile user classification and authorization scheme based on the recognition of user's gesture. Compared to other security solutions like password, track pattern and finger print etc., our scheme can continuously evolve for better protection during the usage cycle of the mobile device. Besides the regular interactive screen and sensors of modern mobile devices, our scheme does not require any additional hardware supports.

Baek-Young Choi – Big Data Transfer Protocols and an Architecture For Clouds; Department of Computer Science Electrical Engineering University of Missouri – Kansas City

The demand for big data transfer is rapidly increasing for applications such as monitoring data transfer, remote site backup, mirroring, and high resolution multimedia content delivery. Traditional data transfer protocols such as TCP need to be enhanced for such big data transfer over modern high speed networks. In this report, we first discuss data transfer protocols proposed for high speed networks as well as cloud data centers, highlighting their key approaches and differences. Based on the insights gained from the protocol study, we then propose a cloud architecture for providing big data transfer as a service that orchestrate big data transfer with other available network and system resources in well planned and scheduled manner.

Mina Guirguis – Control Theoretic Adaptive Monitoring Tools for the Android Platform; Department of Computer Science, Texas State University, San Marcos

With the escalation of attacks that target mobile devices there is an increasing need for efficient monitoring tools. Due to computation, storage, and power constraints of the devices, these monitoring tools may overload the entire system causing severe performance degradation for the running applications. Moreover, they can be pushed by resource-intensive applications and may not perform an adequate monitoring job. To that end, in this project we develop adaptive monitoring tools that are capable of monitoring a wide range of information while efficiently utilizing the available resources on the mobile device. We apply control theoretic techniques to design monitoring functionalities, such as process, integrity and network monitors, that utilize the underlying resources efficiently. This is achieved through controllers that dynamically select the duty cycles of the monitors. Our models and results are validated on the Android platform through emulation and real implementation on the Nexus 7 tablet.

Edwin E. Hach, III – Quantum Mechanical Modeling of Linearly Coupled Waveguide/Ring Resonator Networks for On-Chip Linear Optical Quantum Information Processing; School of Physics and Astronomy, Rochester Institute of Technology

We present an update on our work on quantum optical analysis of waveguides directionally coupled to ring resonators, an architecture realizable using silicon nanophotonics. In this report, we illustrate and discuss, using methods developed in our earlier work, the details of the relationship between the ring resonators systems we examine and the standard Fabry-Perot etalon. We also examine more closely the Hong-Ou-Mandel Trajectories (HOMT), the existence of which we established in out earlier work. Further, we discuss other calculations that we are currently working to complete. These calculations will be central to our scheme for device design. We continue to expect that the results described here will lead to non-trivial, experimentally realizable designs for gates required by LOQC/QIP.

Wei-Da Hao – A Framework Integrated with Wireshark for Network Traffic Analysis Using GPUs in Windows; Electrical Engineering and Computer Science Department, Texas A&M University - Kingsville

This report addresses a framework in Windows for network traffic analysis based on GPU computing under Compute Unified Device Architecture (CUDA). Particularly, the proposed framework integrates with a widely used network traffic analysis tool, Wireshark, to provide an advanced framework for professionals to develop GPU parallel processing.

The processing of network packets is intrinsically parallel, such that network traffic analysis tool inevitably needs to include parallel computing into consideration. While GPU computing gradually becomes main stream parallel computing model, CUDA is currently most effective platform for its development. A similar framework proposed in Linux asks developers to design and develop the program from scratch. It could be a concern that if developer can implement the design effectively within the time constraints. Thus, an ideal framework is one that can utilize both the new features of GPU computing and the existing analysis tool.

The adopted methodology begins from looking into the features of involved software/hardware modules to find out the strategy for integration to construct desired framework. The involved software/hardware modules include CUDA, the installation of CUDA, full CUDA compilation trajectory, the structure of Wireshark, the installation of Wireshark and the compilation of Wireshark. Through the in-depth understanding of CUDA and Wireshark including structures, installations and compilations, we can afford to fine tune these two systems for integration to fulfill the requirement of the targeted framework.

This project successfully identifies the required system parameters to combine CUDA and Wireshark under one framework. Developers can use, on the basis of comprehensive network analysis algorithms, the parallelism of GPU computing supported by the constructed framework to reach the goal of a solution to high performance network traffic analysis.

Chin-Tser Huang – Extending Web Cookies for Management and Analysis of Server-Client Interaction in Cloud Computing; Department of Computer Science and Engineering, University of South Carolina

Cloud computing has attracted plenty of attentions and interests because it realizes the long-desired goal of on-demand network access to a scalable shared pool of computing resources, such as servers, storage, applications, platforms, and networks. However, along with cloud computing also come availability and reliability concerns. As an Air Force Summer Faculty Fellow, the PI's goal is to enhance the reliability and performance of cloud computing by applying cloud auditing techniques to automate the analysis of server-client interactions to ensure high performance of clouds. We had published a paper on a theoretical model which models the interaction between server duties and client obligations as interaction strings, and designed an accountability analysis architecture to monitor and analyze the interaction strings. In the extension project, the PI accomplished three tasks: contributing to a joint TTCP report under Dr. Han's guidance, revising and editing a book chapter, and attending the AFOSR PI meeting in Washington, DC in October 2012. Moreover, we will finish and seek publication of our extended results in an ongoing paper "Snickerdoodle: An Android Cookie Monitoring App".

Murat Kantarcioglu – Novel Access Control Techniques for Large Scale Stream Data Processing; Department of Computer Science, University of Texas at Dallas

Many tasks ranging from cloud auditing to mobile malware detection require large amounts of potentially sensitive data to be collected, stored, shared, and analyzed securely. In addition, in some cases, different data streams coming from heterogeneous sources with different security requirements need to be merged to connect the dots. As an Air Force Summer Faculty Fellow, under the guidance of Dr. Han, we analyzed the data storage and access control needs for cloud auditing and conducted the initial feasibility studies. In addition, we developed initial access control solutions based on storing and processing data on Hadoop[1] platform. Although Hadoop platform is good for batch processing of big data, it is not suitable for online processing of streaming data needed for certain type of audit tasks.

In this extension grant, we developed efficient access control techniques for securely processing large amounts of streaming data. Since our techniques could be implemented without changing the underlying stream processing system, it could be used with minimal overhead.

In this work, we focused on an open source stream processing system developed by Twitter named Storm. Although our proposed ideas are developed with Storm in mind, they are also applicable to other stream processing systems.

Basically, we propose techniques to automatically analyze the sensitivity of a topology used for processing stream data. Based on these automated analysis, each topology could be associated with a sensitivity label. Later on, those labels could be used to define different types of access control policies.

Lifeng Lai – Key Generation in Two-Way Wireless Relaying Systems with Active Attackers; Department of Electrical and Computer Engineering Worcester Polytechnic Institute

Most of the existing work on key generation from wireless fading channels requires a direct wireless link between legitimate users so that they can obtain correlated observations from the common wireless link. In this work, we study the key generation problem in the two-way relay channel, in which there is no direct channel between the key generating terminals. We propose an effective key generation scheme that achieves a substantially larger key rate than that of a direct channel mimic approach. Unlike existing schemes, there is no need for the key generating terminals to obtain correlated observations in our scheme. We also investigate the effects of an active attacker on the proposed key generation protocol. We characterize the optimal attacker's strategy that minimizes the key rate of the proposed scheme. Furthermore, we establish the maximal attacker's power under which our scheme can still achieve a non-zero key rate.

Feng Li – Create Moving Target Defense In Cloud Systems By Learning From Botnets; Department of Engineering and Technology Indiana University, Purdue University

While providing elasticity to clients through on-demand service and cost-effectiveness to service providers through efficient resource allocation, current Cloud infrastructures are largely homogeneously and statically configured for ease of administration. This leaves ample opportunities for attackers to reconnoiter and penetrate the security perimeter of Cloud services.

The research objective of this project is to design a Cloud moving-target defense (MTD) framework. Two facts set the stage for the project: (1) MTD, a promising cyber-security theme identified in the Cyber Leap Year study headed by the Networking and Information Technology Research and Development (NITRD) Program, increases the robustness and survivability of Clouds; (2) Recent advancement in botnet design in response to intense law-enforcement crackdowns leads to successes in evading detection and disruption, and the botnets' anti-crackdown techniques can be reversely used to secure Cloud infrastructures. In this project, four comprehensive and complementary techniques (Heterogeneous VM Replication, Proactive VM Deployment Evolution, Agile Opportunistic Migration, and Dynamic Authentication) are proposed to embody three moving-target defense design principles (diversity, randomization, and authentication) in securing Cloud infrastructure.

Investigation on these four techniques, from the high VM level down to the low networkingdata/ control-plane level, create heterogeneous, continuously shifting Cloud infrastructures, which reduce attackers' understanding of the systems and their ability to launch attacks, while maintaining satisfactory Cloud service performance. Insights from designing, implementing, evaluating the proposed methodology will help build more resilient and trustworthy Cloud infrastructures by diversifying and randomizing the current homogeneous and static Cloud infrastructures without interrupting services. The resulting MTD design and algorithms strike a good balance between cloud service performance and stability in normal situation and cloud survivability under attack.

Seung-Jong Park – Quantitative Performance Evaluation of Assured Cloud Computing Centers Over Ultra-High Speed Networks; Department of Electrical Engineering and Computer Science, Louisiana State University

Large-scale scientific and engineering applications, and cloud auditing generate huge amounts of data. MapReduce framework coupled with cloud computing is emerging as the viable solution for distributed big data processing. Specifically, if data is generated from distributed sources and computation is also distributed then multiple clouds need to be set up to minimize data transfer, which introduces us to federated distributed or multi-domain clouds. As cloud computing has evolved to provide on-demand virtual services and process unprecedented amount of data, many different kinds of cloud computing clusters have been deployed and operated for mission-critical military applications as well as public applications. In case of emergency, it is critical to federate and drive multiple heterogeneous cloud computing clusters, which have been operated by different federal agencies and research institutes. To accomplish time critical missions and succeed a goal, it is necessary to configure software and systems including Hadoop, cloud management software, virtualization software, and operating systems based on the multiple cloud environment and high speed networks.

This project supported from the extension grant of the summer faculty visiting program focuses on the quantitative and qualitative evaluation of performance of Hadoop over distributed computing and high speed network environment after the previous project concentrating on methods to deploy distributed clouds and also to optimize the performance of cloud based applications over such network. The results of performance evaluation and analysis can be used to improve the performance of Hadoop and cloud computing infrastructures over ultra-high speed networks. The proposed work will help not only mission-critical military applications but also future public cloud applications to increase overall performance of assured cloud computing.

Jing Peng – Robust Data Fusion for Target Tracking in Infrared Imagery; Computer Science Department, Montclair State University

Classifiers employed in the real world must deal with various adversities such as noise in sensors, intra-class variations, and restricted degrees of freedom. It is often helpful to develop classifiers that rely on data from various sources (views) for classification. Such classifiers require an effective way of fusing the various sources of information. Resulting fused classifiers can offer a number of advantages, such as (1) increased confidence in decision-making, resulting from fused complementary data, (2) robust performance against countermeasures in battlefield, and (3) improved performance in adverse external conditions. Data fusion finds its applications in many domains such as defense, robotics, medicine, sciences and Space.

Kaliappanadar Ravindran – QoS Auditing for Evaluation of SLAs in Cloud-based Distributed Applications; Department of Computer Science, City College of City University of New York

Given cloud-based realization of a distributed system *S,* QoS auditing enables risk analysis and accounting of SLA violations under various security threats and resource depletions faced by *S*. The problem of QoS failures and security infringements arises due to the third-party control of cloud resources and components that are used in realizing the application-oriented service exported by *S*. The less-than-100% trust between the various sub-systems of *S* is a major issue that necessitates a probabilistic analysis of the application behavior relative to the SLA negotiated with *S*. In this light, QoS auditing allows reasoning about how good the SLA is complied by *S* in the face of hostile environment conditions. The report describes a model-based approach that allows QoS auditing in specific application domains.

Sachin Shetty – Cloud Computing based detection and response mechanism to combat web malware on smartphones; Electrical and Computer Engineering Department, Tennessee State University

The growing popularity and adoption of smartphones has made them a target of malicious activities. The most common malicious activities are targeted towards web-based apps and web browsers on smartphones. Specifically, Blackhat Search Engine Optimization (BSEO) and Social Network Malware (SNM) attacks have infected search results and URLs in smartphones. Recently, static source code analysis of web pages has been proposed to detect BSEO and SNA. However, these approaches are resource intensive and have proven to be impracticable for

smartphone platforms. In this report, we present an approach to detect BSEO and SNM attacks on smartphones by classification of network level features extracted from smartphone traffic on cloud-computing platform. Our proposed approach will leverage the large computational, storage and power resources on the cloud-computing platform to crawl and analyze web pages resulting from BSEO on smartphones.

Sejun Song – Smartphone Cloud for Distributed Data Processing with Applications to Mobile Security and Monitoring; Telecommunications Engineering, Texas A&M University, College Station

Map-Reduce style distributed computation is an integral part of building a smartphone cloud environment. However, traditional cloud system architectures like Hadoop are fundamentally incompatible with smartphones due to bandwidth, memory, and performance limitations. As an Air Force Summer Faculty Fellow, in collaboration with Dr. Han, we have proposed a smartphone-centric cloud approach and prototyped it using Open Service Gateway Initiative (OSGI) architecture. Our goal is to create an efficient and economic Android smartphone cloud platform that 1) enables robust distributed data processing, 2) facilitates modular and dynamic framework, and 3) supports diverse reusable application components.

Alex Sprintson – Design, Development, and Performance Evaluation of Mobile Cloud Computing Systems; Department of Electrical and Computer Engineering Texas A&M University

This report presents the results of my research activities as part of the extension grant given by the Information Institute. My activities included two major thrusts (i) Developing efficient Android cloud computing system; (ii) Robust data exchange in a mobile cloud. We will also outline additional problems related to the distributed key generation that have been formulated in the course of this project.

The goal of the Android cloud computing system is to support robust distributed data processing on mobile devices that leverages the capabilities of the local wireless connections (WiFi and Bluetooth), while minimizing the data movement over long-range and more expensive connections (3G and 4G cellular networks). The system enables efficient access and deployment of applications according to the availability of CPU and user applications.

Nary Subramanian – Natural Language Processing-Enabled Evaluation of Trustworthiness In Software Systems; Computer Science Department, The University of Texas at Tyler

Trustworthiness is emerging as an important requirement for software systems – the National Software Strategy Report has concluded that trustworthiness in software will become the most important goal by the year 2015. NIST has defined trustworthiness in information systems to be systems that are reliable, usable, interoperable, and secure. However, most currently used systems have not been developed with trustworthiness in mind. Therefore, most software systems in use have a trustworthiness "deficit" – that is, they are untrustworthy to a certain extent. This summer we applied the NFR Approach to evaluate trustworthiness in software

systems. The NFR Approach, where NFR stands for non-functional requirements, is a goal-oriented approach wherein goals for trustworthiness are used to evaluate trustworthiness itself. The significant advantages when applying the NFR Approach for evaluating trustworthiness include the ability to apply the method to different definitions of trustworthiness as well as the ability to apply multiple algorithms such as single-value, fuzzy logic, or probabilistic techniques for evaluating trustworthiness.

The NFR Approach treats trustworthiness as a non-functional requirement (NFR) for evaluation. Non-functional requirements are properties that are important for any software system such as trustworthiness, security, reliability, and maintainability. During the process of evaluation, labels, which capture the extent to which trustworthiness is achieved, are propagated up a structure called the Softgoal Interdependency Graph (SIG), where NFR's are represented as softgoals. During this process of label propagation, justifications are used to guide the evaluation process. These justifications are written in a natural language and capture the design decisions/tradeoffs at different points. In order to automate the process of evaluating trustworthiness using the NFR Approach, we plan to apply Natural Language Processing (NLP) techniques to automatically assign labels used to evaluate trustworthiness. As illustrated in the attached figures, NLP will be used to automatically parse justifications and assign labels. Once labels are assigned, the propagation rules of the NFR Approach can be applied to evaluate trustworthiness. We analyzed three NLP tools for this purpose: OpenNLP, CoreNLP, and Natural Language ToolKit, to identify the most suitable candidate for trustworthiness evaluation using the NFR Approach. Based on our study we concluded that the Natural Language ToolKit is the most promising tool for this purpose since it not only provides support for classifying labels but is also platform independent.

Madjid Tavana - The Fuzzy Stability Model: An Interactive Framework for Measuring Robustness and Resiliency under Uncertainty; Lindback Distinguished Chair of Information Systems and Decision Sciences, La Salle University

The increasing complexity in Workflow Management Systems (WMSs) has led to greater vulnerability due to system failure. Although system vulnerabilities cannot be completely eliminated, the accidental or anticipated failures have to be thoroughly understood and guarded. Traditionally, the failure in military Command and Control (C2) systems has been studied with robustness, the concept of self-protecting systems and resiliency, the concept of self-healing systems. Robustness and resiliency in C2 systems are generally measured with precise repair-recovery costs and repair-recovery times. However, the repair-recovery costs and repair-recovery times in real-world problems are often imprecise or uncertain. Fuzzy logic and fuzzy sets can represent imprecise or uncertain information formalizing inaccuracy in human decision-making. We develop a stability model for simultaneous consideration of robustness and resiliency in fuzzy C2 systems. We measure robustness and resiliency with fuzzy repair-recovery times and fuzzy repair-recovery costs. The interactive method plots the fuzzy robustness and fuzzy resiliency measures in a Cartesian coordinate system and derives an overall *fuzzy stability index* for various processes in the C2 system based on the theory of displaced ideals.

Dmitry Uskov – Designing Optimal Schemes For Photonic Cluster Sate Generation; Division of Mathematics and Science, Brescia University *and* Department of Physics and Engineering Physics, Stern Hall Tulane University

We performed numerical and analytical analysis of the problem of photonic cluster-state generation in application to quantum computation technology. We suggested a new scheme of multiphoton cluster state generation. The scheme provided the most efficient method of cluster state generation and allows using type-I SPDC as a brighter source of photons without any loss of the efficiency in cluster generation. Optimization tasks performed by us are of crucial importance for photonic quantum computation since the only photon-photon entangling operations implementable currently in a lab are measurement-assisted stochastic quantum transformations. Our theoretical results demonstrate that previous methods of cluster state generation are by far not the optimal one. Performing numerical optimization we discovered a new scheme of cluster state generation which boosts the success rate of generation by more than an order of magnitude even for a small eight-qubit cluster state. The advantage of our scheme in comparison with traditional schemes grows exponentially fast with the size of cluster. Next, found a general analytical method of optimizing cluster state generation which expands our abilities of designing simple experimental setups for realization of our technology in practice. We expect that future experiments with photonic clusters will be exploiting our schemes to provide the most efficient realization of linear optical quantum information technology.

Jonathan White – Multi-modal Sensors for Survivability Prediction of Mobile Devices: Sensor Simulation and Experimentation; Department of Engineering and Physics, Harding University

This report details the work that was done in order to improve the survivability of mobile devices that are equipped with multi-modal sensors. Commercial off-the-shelf (COTS) mobile communication devices are being used much more frequently by warfighters throughout the DOD and this expansion has motivated the need for this work. Multi-modal sensors on mobile devices are able to detect both the physical and logical environment and by combing data from both, a more accurate prediction of the survivability model can be developed, enabling the warfighter to replace their low-cost COTS device with another device before it fails. To our knowledge, the usage of both hardware and software sensors to inform a survivability model on a COTS mobile device has never been tested before. This survivability data increases the utility of the COTS device to the warfighter in the field, as our results will affirmatively show. This report primarily details the sensor simulation and experimental design; the system model, filter design, and prediction model are being designed by other researchers on the team. The report details several simulations that are run and results are presented that demonstrate how the proposed model works using several different multi-modal sensor inputs and several different simulation parameters.

Chengshan Xiao – Interference channel exploitation and secure communications in wireless links; Department of Electrical and Computer Engineering Missouri University of Science and Technology

In this project, we have $\log_2 M_1 + \log_2 M_2 + \cdots + \log_2 M_K$ investigated the linear precoding design for multi-user multiple-input multiple- output (MIMO) interference channel systems. To break away from the traditional studies based on idealistic Gaussian input assumption, we formulated the problem of maximizing mutual information for finite alphabet inputs. We derived the achievable rate expression of each user. Our analysis at the high signal-to-noise ratio (SNR) revealed that the well-known interference alignment (IA) technique designed for Gaussian input case will lead to a significant sum-rate loss due to the utilization of partial interference-free signal space for transmission. In light of this, we have developed an efficient power allocation scheme designed for finite alphabet input scenario at high SNR. The proposed scheme achieves the analytical upper-bound sum-rate of the entire signal space, b/s/Hz under finite alphabet constraints. More generally, we derived a set of necessary conditions for the WSR maximization precoding design based on Karush-Kuhn-Tucker (KKT) analysis, from which we developed an iterative algorithm for precoding optimization. We applied gradient descent optimization and used backtracking line search algorithm to regulate the convergence speed. Our tests, based on low-density parity-check codes (LDPC) coded quadrature amplitude modulation (QAM) signals in the multi-user MIMO interference channels established the coded BER performance of the obtained linear precoders. Our numerical results demonstrate that the proposed iterative algorithm achieves considerably higher sum-rate under practical QAM inputs than other known methods.

Kaiqi Xiong – An Efficient Approach for Detecting and Measuring Black Hat SEO Attacks on Smartphones; Department of Computing Security, Rochester Institute of Technology

Mobile devices such as smartphones have been significantly starting to change our daily life. While they help us keep connected to the world anywhere and anytime, the connectivity and accessibility has raised many security challenges. Black Hat Search Engine Optimization (SEO) attack is one of such challenges on smartphones. It employs techniques to increase search rankings in an unethical manner, which is dramatically harmful to smartphone users and providers. The goal of this extension project is to explore and investigate an efficient approach for detecting and measuring black hat SEO attacks on smartphones. We propose a mobile cloud-assisted technique for tackling the detection and measurement of black hat SEO attacks. Specifically, we develop a systematic method for clustering and classification smartphone web traffic traces via clouds by using novel genetic algorithms. The proposed method provides us a globally optimal solution of this parallelization problem. Its feasible and effective implementation is discussed in detail. The resulting efficiency and accuracy is superior to the ones obtained by a use of those approaches in which this problem is divided into the two parts: location and allocation, respectively. The cloud-assisted method is used for detecting and measuring black hat SEO attacks on smartphones.

Shouhuai Xu – Real-Time Detection And Prevention Of Android Permission Abuses; Department of Computer Science University of Texas at San Antonio

Android smartphones are widely used, while their security remains to be a technical challenge. Android permission system is an important component of the Android platform. It was designed with the aim to help smartphone users manage the permissions (privileges) that are granted to Android applications (apps). Basically, the permission system can inform human users about the privileges that are demanded by apps at their installation time. In principle this would allow the users to assess the potential risk of installing the apps, and there determine whether to install the apps or not. Unfortunately, recent studies showed that the installation-time permission management function is often ignored, simply because users often did not pay attention to the permission system or did not understand the permission system. As a consequence, malicious apps are often granted with security- and privacy-critical permissions, which can be abused to launch attacks without being noticed by the human users. In this report, we describe the design, analysis, and implementation of a novel solution to mitigating the consequences caused by permission mismanagement. The solution, called AnDroid Permission Abuse Detector (DroidPAD), aims to detect and prevent abuses of Android permissions in real-time. The key idea underlying DroidPAD is the leverage of system- and application-level context information. A preliminary evaluation shows that DroidPAD detected and prevented permission-abuse activities with high accuracy, low false-positive rate (3.1%), and zero false-negative rate.

Tianyu (Thomas) Yang – Efficient Adaptive Techniques in Wireless Receivers for Frequency-Selective I/Q Equalization and Digital Beamforming under Time-varying Channel Environments; Department of Electrical, Computer, Software and Systems Engineering, Embry-Riddle Aeronautical University

This extension grant project continues the study of adaptive signal processing techniques in I/Q equalization and digital beamforming applications. Specifically, the online recursive I/Q equalization method proposed during VFRP 2012 was extended to the multi-tap version in order to better combat frequency-selective mismatches in wideband receivers. For interference suppression in digital beamforming receivers, to further investigate the effectiveness of two adaptive algorithms developed during VFRP 2012, they were evaluated in time-varying wireless channels to study the performance of the new techniques in practical mobile communication scenarios. MATLAB simulations indicate that, the multi-tap version of the I/Q equalization method achieves image suppression over a wide frequency band in the presence of frequency-selective mismatches, and the two proposed adaptive beamforming techniques maintains satisfactory interference suppression performance and convergence properties under time-varying channel conditions.

Janusz Zalewski – Development of Security Assessment Methods for Cyberphysical Systems; Computer Science and Software Engineering Programs, Florida Gulf Coast University

This project, being an extension of the Summer 2012 VFRP Faculty Fellowship, studied additional issues related to modeling and analysis of trust attributes in software. In particular, it

attempts to contribute to the development of security assessment for cyberphysical systems. It continues the summer project in the following aspects:

1) Developing a process for security assessment in cyberphysical systems.

2) Applying the process and the specific model of a trustworthy architecture to developing new Case Studies suitable for conducting the analysis and assessment of aspects of trustworthiness.

3) Using the case studies to analyze models of security and trustworthiness, with automatic modeling tools, for wireless network standards, such as RFID and Zigbee.

With respect to (1), a preliminary experimental process has been established and applied to two essential examples of cyberphysical systems: an industrial control system (ICS) such as SCADA, and an expanded ICS imitating a smart grid component of the critical infrastructure. The use of penetration tools, such as Metasploit, Wireshark and others, was fundamental in accomplishing this step.

Regarding (2), a case study has been developed, based on the information collected in step (1), to assess security properties quantitatively with the application of the Common Vulnerability Scoring System (CVSS). A related paper is scheduled for presentation at the CSIIRW 2013 - 8th Annual Cyber Security and Information Intelligence Workshop, in Oak Ridge, Tenn., January 8-10, 2013.

With respect to (3), two models of wireless sensor networks, one based on RFID (ISO/IEC PUB 18000) and another one based on Zigbee (IEEE Std 802-14.5), have been briefly analyzed with respect to security assessment. The RFID network has been modeled on a real equipment and the Zigbee network has been simulated using the NetSim tool.

Finally, based on the results of the modeling, recommendations have been made to expand the study towards more extensive research of security assessment in wireless networks and include higher software layers pertaining to security, involving: (1) an operating system, such as Android, and (2) a programming language, for example, Java. It is also essential to continue studies on theoretical underpinnings of security assessment in cyberphysical systems, based on reasoning about uncertainty, with applications of non-statistical, such as Bayesian networks, rough sets or equivalent.

Qiang (Martin) Zhao – Situation Identification and Threat Assessment (SITA); Department of Computer Science, Mercer University

Works of this quantification effort (code named as Situation Identification and Threat Assessment (*SITA*) *Boom!* or *"How well can we identify threat left of boom?"*) started in summer 2012 with a discussion on its purposes and overall objectives. As illustrated in Figure 1, with sensory data (such as Intrusion Detection System (IDS) alerts) and additional event tracking and analysis (such as using Information Fusion Engine for Real-time Decision-making (*INFERD*)), one can only detect an intrusion or attack and determine the damages that it makes after it has already happened. It is of great interest to a decision maker to predict an upcoming threat and its impacts before it occurs.

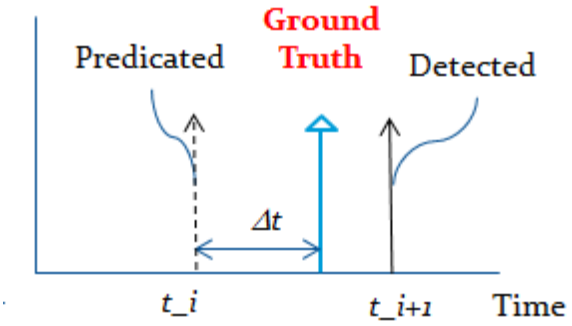

Figure 1 – Illustration of *"How well can we identify threat left of boom?"*

Based on the SA reference and process models proposed by AFRL/RIED researchers, the *SITA* system is designed to provide these prediction capabilities based on the knowledge of "us" (our missions and the supporting assets, our vulnerabilities and possible damage propagation trends, etc.) and knowledge of "them" (adversary characteristics, such as their past behavior, capabilities/capacities, and opportunities). More specifically, the inclusion of algorithms dealing with adversary characteristics into the Threat Identification and Assessment (TIA) loop can identify "plausible" futures among all "possible" future states based on the vulnerability structure for "the" mission.

However, the inclusion of these algorithms may be a double-edged sword: On the one hand, they may help improve the plausibility of the projected futures; but on the other hand, if the processing time tends to be too extensive, there will not be enough response time before an attacker strikes. Therefore, this R&D project's main objective is to explore ways to pin-point when *SITA* first projects a future state that reveals the adversary's goal state (assuming there's a projection at all). It also tries to measure the effectiveness of the proposed algorithms and tools (for modeling adversary characteristics) and carry out cost-benefit analysis. The essential approach is to monitor and analyze the progression of Java Messaging System (JMS) messages passed among *SITA* components for a set of given test cases and to check against the onset of known goal states.

Lizhong Zheng - Managing Big Data With Sparse Structures; Department of Electrical Engineering and Computer Sciences, Massachusetts Institute of Technology

Currently, the research on big data is an active topic. As the technologies evolve, one can envision that information managed in a normal battlefield scenario will soon fall in to the category of big data. That is, there will be all kind of different information gathered from different kind of sensors, or data bases, that need to be interpreted, processed, transmitted, restored, in real-time. On the other hand, the time we have for such processing is at least not increased, if not cut even shorter by the fast pace of the military actions. This not only presents new challenges in the communication networks to carry these data, but also leads to challenges in computation and storage, which are traditionally not in the realm of information theory studies. In this project, we discuss the new theoretically tools to handle such problems. In particular, we emphasize on two aspects of the problem. First, we study the schemes that can take the advantage of the statistical structure of the data, in particular, graphical models or

sparsity, which can be used to greatly simplify computation and improve the quality of local processing; secondly, we try to come up with a framework which view the assumption of a sparse model as willingness of losing some aspects of the data, and understand the fundamental limits of lossy processing based on selection of features in data for communication, fusion, and storage for unpredictable future uses.

4. EXPENDITURES

Under this contract expenses were billed on a faculty/week basis. The rates for the professors were established by the National Research Council for summer research fellows and are as follows.

4.1. Faculty Labor

Assistant Professor	$1,300/week
Associate Professor	$1,500/week
Full Professor	$1,700/week
Faculty Per Diem:	$50/day up to $250/week

*Faculty members whose home residence/university is more than 50 miles from AFRL/IF were entitled to Per Diem

4.2. Other Costs Associated with Program

Round trip travel reimbursement at the start and completion of the project was provided as requested to faculty and students.

Housing and meal allowance - SUNY/IT dorm fees

Administrative Assistant Salary and Fringe Benefits

Conference Registration Fee – Faculty and Student Cyber Information Challenges Conference

Laptop Air Card

Advertisement for Admin Assistant Position

Finger print fee and postage for one student

Heather Dussault salary and fringe for Cloud Workshop 2011

5. LIST OF ACRONYMS

2D – Two dimensional

3D – Three Dimensional

3D IC –

3G – Third Generation

4G – Fourth Generation

AB – active bundles

AFOSR – Air Force Office of Scientific Research

AFOSR PI – Air Force Office of Scientific Research Principle Investigator

AFRL – Air Force Research Laboratory

AFRL/RL – Air Force Research Laboratory/Research Institute

ARS – Autonomous robotics system

ASC – Android Smartphone Cloud

BSEO – Blackhat Search Engine Optimization

C2 – Command and Control

CAN – Controller Area Network

CDN – Content Distribution Network

CMOS – Cellular Management Operation System

COTS – Common off the shelf

CPU – Central Procesing Unit

CRN – Cognitive Radio Network

CS – Compressed sensing

CUDA – Compute Unified Device Architecture

CVSS – Common Vulnerability Scoring System

CW – Continuous wave

DDoS – Distributed Denial of Service

DIIM – Discover, Identify, and Introduce Model

DoD – Department of Defense

DroidPAD – AnDroid Permission Abuse Detector

ECOPS – Energy-Efficient Cooperative and Opportunistic Positioning System

EOARD – European Office of Aerospace Research & Development

FaaS – File Transfer as a Service

FFD – First Fit Descending

FOBS – Fractional Orbital Bombardment System

FRTP –

GPS – Global Positioning System

GPU – General Processing Unit

GVOWOT – generalized variable overlapped window orthonormal transform

HOMT – Hong-Ou-Mandel Trajectories

I/Q – Inphase and Quadrature

IA – Interference alignment

IBM – International Business Machines Corporation

ICS - industrial control system

IDS - Intrusion Detection System

IEEE – Institute of Electrical and Electronics Engineers

INFERD - Information Fusion Engine for Real-time Decision-making

IP – Internet Provider

IP ID – Internet Provider Identification

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission

JMS – Java Messaging System

KCQ – Keyed Communication in Quantum Noise

KKT – Karush-Kuhn-Tucker

LCD – Liquid Crystal Display

LDPC – Low-Density Parity-Check codes

LOQC/QIP - Linear Optical Quantum Computing/Quantum Information Processing

MATLAB – Matrix Laboratory

MIMO – Multiple-Input Multiple-Output

MIO – Managed Information Object

MIS – Metal-Insulator-Semiconductor

MOS – Metal-Oxide-Semiconductor

MTD – Moving-Target Defense

N-CET – a tracker

NetFPGA – Network Filed-Programmable Gate Array

NFR – non-functional requirement

NITRD – Networking and Information Technology Research and Development

NLP – Natural Language Processing

NMS – Network Management System

NY – New York

OSGI – Open Service Gateway Initiative

PI – Principle Investigator

QAM – Quadrature Amplitude Modulation

QCA – Quantum cellular automata

QoS – Quality of Service

R&D – Research and Development

RF – Radio Frequency

RFID – Radio Frequency Identification

SA – Situation Awareness

SABUL – Simple Available Bandwidth Utilization Library

SCV – Space Construction Vehicle

SIG – Softgoal Interdependency Graph

SITA – Situation Identification and Threat Assessment

SLA – Service Level Agreement

SNA – Systems Network Architecture

SNM – Social Network Malware

SPDC – Surge Protective Devices Committee

SPIE – International Society for Optical Engineering

SPNE – Subgame Perfect Nash Equilibrium

STD – Standard

STRIDE/DREAD – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (mnemonic for threats to software, used to make threat-modeling scenarios) / Damage potential, Reproducibility, Exploitability, Affected Users, Discoverability (threat modeling)

SVI – Survivable Virtual Infrastructure

SWDR – Software Defined Radio

TCP – Transmission Control Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

TIA – Threat Identification and Assessment

TSEC – Trusted Computer System Evaluation Criteria

TSV – Through Silicon Via

TTCP – Test Transmission Control Protocol

UDP – User Datagram Protocol

UDT – Uniform Data Transfer

US – United States

USC – University of South Carolina

VFRP –Visiting Faculty Research Program

VLM – Virtual Link Mapping

VM – Virtual Machine

VMP – Virtual Machine Placement

VOWOT – Variable Overlapped Window Orthonormal Transform

WAN – Wide Area Network

WiFi – Wireless Fidelity

WMS – Workflow Management Systems

WPAFB – Wright-Patterson Air Force Base